Faculty of Social Sciences

MSc in International Public Management and Policy

Lobbying success in EU digital policy

Master Thesis

19 June 2020

1st Reader: Prof.Dr. M. Haverland

2nd Reader: Dr. A. Zhelyazkova

Author: David Keane

Student number: 498384

Word count: 19,957 (including graphs and tables)

Abstract

The digital economy has undergone one of the largest transformative changes since the beginning of the twenty-first century. The European Union has responded to this development introducing a series of policies under the framework of the EU digital single market. While there is a growing body of literature explaining the involvement of interest groups in Brussels, few have looked at what interest groups are succeeding in the realm of digital policy. This research provides a case study on interest group involvement on two EU proposals, the data protection regulation (GDPR) and cyber security directive (NIS) to understand what explains the success of interest groups in EU digital policy. From analysing popular theoretical approaches on explaining influence, elements of issue-specific characteristics, interest group characteristics and institutional factors are used to explain why some interest groups out-perform others and how underperforming groups can improve their position. This research uses the preference attainment method in measuring preferences of interest groups by adapting a quantitative design to suit a case study research. The results indicate that public salience of an issue is an important factor to consider in certain institutional contexts when measuring the success of interest groups. The research supports a common school of thought in the literature which indicates the dominance of private interests over public interests with respect to EU digital policy. However, NGOs can improve their position by understanding explanatory factors of success outlined in these two proposals to adjust their strategies to improve their outcome.

Acknowledgements

Firstly, I would like to thank my thesis supervisor, Prof.Dr. Markus Haverland, for his expertise and teachings throughout this process. I would like to thank my second reader Dr. Asya Zhelyazkova for her guidance and feedback this year. I am grateful to my thesis circle friends Joan Viscarro, Katharina Ruppert, and Stefan Koster for their constructive feedback and positive support in every meeting. I extend a special thank you to Mairead Fanning for her amazing support during the year in both an academic and personal setting. Finally, I would like to thank my parents, Tom and Jane, my sister Adèle and boyfriend Cormac for their continued love and support always.

Table of Contents

List of Tables

List of figures

1. Introduction

There has been a global revolutionary change over the past thirty years thanks to technological advancement. Technology has truly transformed from an abstract cinematic sci-fi phenomenon to a taken-for-granted facet of everyday life. Many scholars claim that we are living in the "digital age" with some labelling it "the fourth industrial revolution" (Schwab, 2015). Whatever the terminology, digital infrastructure is a cornerstone of today's society. Business, education, healthcare and social interactions have changed through digital infrastructure. It is affecting politics and our laws. Technology is a disruptor to society with new inventions and processes emerging at an increasing rate which creates difficulties for lawmakers and international institutions that are playing a game of catch-up to innovators. For example, social media platforms are advanced technological disrupters to society that are consistently updated and adapted to a changing environment. Facebook's interface, functionality and issues it generates are virtually unrecognisable today compared to how it looked when it was first created (Malan, 2018). Once regulators address data privacy issues created by Facebook through a long legal bureaucratic process, the policy quickly becomes irrelevant as the platform is transformed, presenting new issues for regulators to understand (Malan, 2018). As digitalisation dominates society, lawmakers worldwide have reacted with attempts to regulate the digital infrastructure in which we operate and restrict the power of those providing the technology without stifling innovation.

The European Union has been one of the most proactive political powers in introducing legislative procedures to regulate the digital economy. Within the past ten years, the EU has introduced a series of new laws aiming to strengthen Europe's digital single market and act as a pioneer for creating policy to regulate technology. Areas of specific concern have focused on data protection, e-privacy, copyright and cyber security to name but a few.

The technological revolution has affected interest group lobbying in Brussels which has expanded rapidly over the past ten years. Many American "big-tech" private interests, who provide most of the digital platforms we use, have flocked to Brussels investing a large sum of

revenue in lobbying activities to ensure their voices are heard and that their interests are protected. Since 2014, "big-tech" interests lobbying Europe has increased by 278% (Cooper & Hirst, 2017). Many studies give reasons why arguing that business interest lobbying has increased as the EU is creating more legislation which directly impacts corporate affairs (Harris & Lock 1996; Levitt, Bryceson & van Mierlo 2017). NGOs representing public interests have also reacted to this change with many digital oriented NGOs being created to ensure private interests do not dominate the development of EU digital policy. They advocate for civilian participation in the regulation of technology, ensuring power is evenly distributed. Interest groups represent private and public issues across many sectors, countries and people affected by the technological revolution. While there is plenty of research conducted on the effect of lobbying on European affairs, little research has been done to examine what groups are participating in shaping EU digital policy and what groups are succeeding in achieving their desired outcome. From a theoretical standpoint, this research addresses this gap in the literature by examining causal factors of interest group success with respect to recent EU digital policy proposals.

1.1 Research aim and question

There is a growing work of literature which suggests that interest groups are playing a greater role in shaping and supporting EU legislation within the last twenty years, especially those representing private interests as evidenced by the increase of ''big-tech'' lobbying (Coen, 1997; Levitt, Bryceson & van Mierlo 2017; Atikcan & Chalmers, 2019). Much research has been conducted to establish theories and causal factors which explain why certain interest groups are succeeding relative to other groups. As demonstrated in chapter 2, some argue that business interests are shaping policy whilst others insist that public-interest groups, NGOs, are just as capable as influencing the legislative outcome (Mahoney, 2007; Baumgartner, Berry & Hojnacki, 2010). To help explain why this is, academics focus on different approaches that describe what causes "influence of interest groups". In this research, this refers to an interest group's ability to achieve its own preferences in a policy proposal. Eising (2007) and McKay (2012) are examples which argue that research should focus on examining characteristics of interest groups themselves whereas others look at issue-specific characteristics of policy proposals to explain why certain groups are winning in legislative proposals (Mahoney, 2007;

Kluver, 2011). Other arguments such as Bouwen (2002) put great emphasis on the characteristics of the three main EU institutions: The Commission, the Council of Ministers, the European Parliament, henceforth referred to as the Council and the Parliament respectively. This research adds to the academic discourse by examining aspects of these approaches by applying them to the case of EU digital policy to understand what groups are influential and achieving their desired outcome. Therefore, this research will examine important elements of characteristics of interest groups, the issues that occur during the legislative proposal and interest group performance at the three main EU institutions to understand who is achieving their desired outcome and why that is the case. With this foundation, the following research question has been formulated:

To what extent do interest group characteristics, issue-specific characteristics and EU institutional factors explain how interest groups achieve their preferences when lobbying for EU digital policy?

This research derives several hypotheses to test what factors explain interest group success in EU digital policy making. The hypotheses are derived from theory examined in the literature review, chapter 2, and the theoretical framework, chapter 4. As this research examines the influential capacity of business interests compared to NGOs, hypotheses will be developed to analyse this and add to the literary discussion. The research is conducted through a co-variational (COV) case study to provide a succinct and valid answer to the research question.

1.2 Societal relevance

This research provides several implications for society. Initially, society should be aware of the main actors who shape legislative policy at the EU. Hix & Hoyland (2011) illustrate that the EU has created an open platform for NGOs, business associations, private firms, think tanks and educational institutes to participate in policymaking at European level. This can be reflected in the 8,000 interest groups registered on the ‘‘EU Transparency register’’ (Europa, 2020) which grants groups access to EU decision-makers. Interest group representation is an important element of EU politics. Second, building on this, interest groups should be aware of what channels work best to exert influence in developing EU digital policy. As this research focuses on lobbying efforts across the three EU institutions, NGOs and business associations can understand what institutions respond well to their cause and how they can improve their outcome

in the legislative process. Third, technology's role in society and politics has caused much controversy in recent years. Reports of MEPs directly copying and pasting requirements from tech giants into their proposals raises an eyebrow to the growing influence of big-tech interests' in European politics today (Atikcan & Chalmers, 2019) From the citizens' standpoint, it is important to understand who is being heard in Europe and if it reflects the opinion of the public.

1.3 Theoretical relevance

This research has several theoretical implications which can improve the academic literature. First, while there have been many advances made on EU lobbying literature in recent years, few have addressed the topic of digital policy. Interest group participation in the digital single market is an important development of EU policy over the past decade which begs further analysis to provide more cases as examples of how EU policy is made. Second, as the literature demonstrates, there are several approaches used to explain interest group success in Europe (Coen, 1997; Bouwen 2002; Mahoney, 2007). Scholars debate whether interest group characteristics, issue-specific characteristics, institutional factors or a combination of all three best explain the performance of interest groups. This research provides an answer to this question with respect to digital policy whilst adding to the discourse on interest group literature.

Third, this research examines the effectiveness of established research designs with respect to interest group success. This research analyses why Dür's (2008) preference attainment method is an appropriate method for case study research. Furthermore, this research applies the preference attainment method by combining research frameworks provided by Mahoney (2007) and Bunea (2013). This provides a new approach in measuring interest group success in a qualitative study. Finally, this research looks at how theory can be used to explain how interest groups perform differently at the three main EU institutions and why it is important to consider all institutions of the EU when lobbying.

1.4 Research structure

The research is presented as follows. Chapter 2 provides a background to lobbying, analysing approaches that were developed in a U.S. context and adapted to the EU. It then focuses on the main approaches to explaining interest group representation in Europe. Chapter 3 introduces the three main institutions and their roles in the legislative process. Chapter 4 presents a theoretical

framework derived from the literature explaining appropriate factors to measure, which helps in explaining what interest groups are performing well in lobbying. Several hypotheses are developed based on interest group literature which covers issue-specific characteristics, interest group characteristics and institutional factors. Chapter 5 presents the research design and units of analysis that are used. It discusses available methods and units, a justification for the chosen method and units and a walkthrough on how they are applied to the case. It then discusses data collection for analysis. It provides information on the type of documents used and justifications as well as obstacles that occurred in finding data for this research. Chapter 6 provides an overview of the cases and their main issues which were important to interest groups. Chapter 7 provides an analysis using the methodological steps outlined in chapter 4. Chapter 8 provides a discussion and testing of the hypotheses against the analysis. Finally, chapter 9 provides an answer to the research question and recommendations for interest groups interested in lobbying for digital policy.

2. Literature Review

The literature review gives an overview of the academic discussion on interest groups. This review looks at theories conceptualised in a U.S. context which were later adapted to EU politics through case studies and quantitative analysis. The review arrives at three schools of thought in explaining influence of interest groups. Finally, it looks at interest group type arriving at a gap in the literature which will be addressed through the theoretical framework.

2.1 Origins of lobbying

Interest group literature dates to the 1920s focusing on case studies in the United States (Woll, 2006). According to Woll (2006), there have been four seismic changes or "waves" in lobbying documented in literature. Truman (1951) provides a starting point for this discussion where he looks at the role of non-state actors that apply "pressure" on government institutions to achieve the desires of the people they represent. He analyses various relationships of different groups and interest coalitions within the American political environment. This eventually led to theories being conceptualised specifically on interest groups. Traditionally, interest groups are generally divided into two groups: those representing private interests and those representing public or "diffuse" interests (Beyers, Eising & Maloney, 2008).

Pluralism is one of these theories that emerged. According to the pluralist argument, there is an interest group on every side of an issue (Hix & Hoyland, 2011). It is a normative argument, suggesting that all interest groups have equal representation and equal access to decision-makers. However, through research contradictory arguments to the pluralist approach have emerged (Olson, 1965; Maloney, Jordan & McLaughlin, 1994). Mancur Olson (1965) highlighted flaws with this normative approach to studying interest groups through developing the theory of collective action. According to this theory, interests that represent few members will be overrepresented and larger, public or "diffuse" interests will suffer as a result. This results in the free-rider problem that occurs when a group becomes larger. A free-rider problem is a market failure that occurs when those who benefit from goods do not provide resources in attaining these goods. This is the case for public goods which do not exclude access for anyone unlike private goods which are enjoyed by members who paid for them only (Olson, 1965).

Since the Single European Act in 1986, there has been an explosion of literature focusing on lobbying success at EU level in Brussels (Cown, 1997; Greenwood 1997; Bouwen 2002; Michalowitz, 2002; Eising 2007; Mahoney 2008; Kluver 2011). Many of these academics expanded on theories outlined above to analyse the case of interest group influence at EU level. The rest of this review will discuss this development.

2.2 Theories explaining influence

There is a debate on what factors explain lobbying success. Mahoney (2007) and Dür & de Bièvre (2007) discuss three approaches that are important to explain what or who influences the outcome of policies through the legislative process. They are issue-specific factors, interest group characteristics and institutional factors. Issue-specific refers to important factors of issues that occur during the creation of legislation that affect an interest group's ability to exert influence (Mahoney, 2007; Kluver, 2011; Baumgartner, Berry, Hojnacki & Leech, 2010). Interest group characteristics refer to the permanent and non-permanent characteristics of the interest groups themselves which can be factors that explain influence (Coen, 1997; Eising, 2007; Michalowitz, 2007; McKay, 2012). Permanent characteristics refers to fixed attributes of the group that do not change subject to the issue they are lobbying. Certain characteristics, such as finance, can change over time as a group accumulates or loses wealth however usually remains fixed over long periods of time. Non-permanent characteristics refers to temporary

attributes that a group possesses which are circumstantially relevant. For example, a group representing the banking industry is expected to possess expert information when dealing with financial policy but loses this attribute for environmental policy. The possession of this characteristic is non-permanent. Institutional factors refer to the characteristics of the EU institutions themselves and their relationship with interest groups (Michalowitz, 2002; Bouwen 2002). These three approaches will be taken in turn.

2.2.1 Institutional context of the EU:

There is evidence that suggests the characteristics of the EU's main institutions can explain patterns of influence of interest groups and explain why some are more successful in achieving their preferences. The EU institutions are not as well-resourced or staffed as national governments and require outside assistance to supply them with resources to legitimise their standing (Greenwood, 2007). Bouwen's access theory (2002) discusses the resources required by EU institutions for interest groups to gain access. The group that can effectively provide these resources will have greater access to the EU institutions which leads to greater success for that group.

Bouwen (2002) demonstrates that through the logic of access, interest groups will perform differently depending on the European institution they lobby. This is based on a supply and demand economic model whereby each institution requires different access goods from interest groups. Some interest groups are better equipped to supply goods to one institution over another. The Commission and Parliament are relatively responsive to European association groups as evidenced by interest groups gaining access to these institutions through the transparency register (Michalowitz, 2002). Coen (1997) and Eising (2004) illustrate that the Commission requires expert knowledge to improve policy proposals which business interests are easily able to supply. This highlights a flaw in the pluralist argument as not all groups have equal access to institutions. Neo-pluralism is used to explain why the EU provides resources to those representing diffuse interests to countervail the power of private interests (Hix & Hoyland, 2011). However, mounting evidence suggests that private firms are more successful in targeting the multilevel structures of the EU (Olson, 1965; Coen 1997; Bouwen 2002; Hix & Hoyland, 2011).

Michalowitz (2002) demonstrates that the Parliament welcomes and encourages participation from interest groups. Interest groups provide a valid source of technical information which the

parliament needs to make amendments on legislative proposals, reducing its reliance on other European institutions. Using access theory, European associations that build consensus positions of their members are likely to be successful at the Parliament (Bouwen, 2002). Neither author specifies whether business interests or NGOs are more successful at the parliament. Hix & Hoyland (2011) present arguments when ‘‘Members of European Parliament’’ (MEPs) are likely to support business interests. They suggest that when voters are “rationally ignorant” about specific policy details, it allows MEPs to vote in line with private interests as these groups can supply resources to help MEPs get re-elected (p. 191). Hix and Hoyland (2011) remind the reader that MEPs are career driven and usually have two other goals in Parliament; to satisfy the ideological values of their national party and please European Parliament committees and leaders if they seek senior roles within the Parliament (p. 55).

The multi-level institutional structure of the EU is unique and its relationship to interest groups should be examined. Greenwood (2007) illustrates that the three main branches of EU legislation require input from lobby groups whereas Bouwen (2002) argues that national associations based in the member state capitals usually enjoy a strong relationship with their government and have better access to lawmakers at national level. They are most likely to have their interests met at the Council. Michalowitz (2002) agrees with this calling for interest groups interested in lobbying the Council to take their activities away from Brussels and focus on member state capitals instead. Although different rules apply for each venue, the literature illustrates an opportunity for interest groups to be influential on multi-level platforms.

2.2.2. Issue-specific approach

Lowi (1972) illustrates that many issues occur in creating legislation. This can affect an interest group’s ability to exert influence and achieve their preferences. They can differentiate from distributive issues which focus on fixed resources that must be divided between two or more parties and regulatory issues which enhances or restricts the capabilities’ of individuals and groups, with the aim of achieving a desired behaviour of that group. Regulatory policies can be used to correct undesired actions through punishment and sanction. Research claims that private interests are more influential in distributive issues as there is less opposition compared to regulatory issues (Eisling, Rasch & Rozbicka 2017). Other types of issues range from simple, complex, conflicting and salient issues. Mahoney (2007) and Klüver (2011) examine the latter

two in the context of interest group lobbying in Brussels arguing that as salience increases, the less successful individual advocates should be in lobbying as there are more stakeholders. Klüver (2011) argues that the degree of conflict on an issue is an important causal factor of influence. Conflicts usually have two sides, pro and against. The larger coalition on the conflict is more likely to achieve their desired outcome. Michalowitz (2007) looks at three factors necessary for interest groups to exert influence in the EU legislative process. Michalowitz (2007) agrees with this theorising that where degree of conflict between groups is high, influence will be difficult to exert however where there is little conflict, influence on the outcome will be more likely.

Scope is another issue-specific factor to consider. Mahoney (2007) argues that as the number of actors seeking their preferences on an issue increases, the ability to achieve their preferences decreases. This occurs in distributive issues where more voices must be satisfied (Lowi, 1972). Private firms can more easily exert influence on niche and sector-related issues (Eisling, Rasch & Rozibicka 2017). Public salience and scope outlined by Mahoney (2007) are linked. Policymakers feel it is unwise to focus their attention to one group, specifically private interests, and involve multiple actors in developing legislation fearing scrutiny from the public (Mahoney, 2007). Democratic institutions must appear to represent the public they serve, rather than a single private interest especially when under the scope of the media who will document any favouritism towards private interests over the public. Culpepper (2011) agrees with this research who argues the narrower an issue is and the less public attention it receives the more likely private firms can exert influence and achieve their outcome.

2.2.3. Interest group characteristics:

This section looks at an array of characteristics of interest groups themselves and how they have been used to explain interest group success in Europe. Bouwen (2004) states that interest group success will differ across the Commission, Council and European Parliament due to the resources that they possess. Using the logic of access (Bouwen, 2002) interest groups use their resources to gain access to EU institutions. Bouwen (2004) concludes that not all interest groups can possess the access goods required by the institutions and therefore success of interest groups depends on its own resources and the institution that it lobbies. As already illustrated, interest group characteristics can be permanent, such as group type and finance or non-permanent such

expert information which can vary depending on the legislative proposal. This review will initially look at permanent characteristics.

Interest group type is an important factor explaining influence. The two groups examined here are those representing private interests represented by business associations and public interests represented by NGOs. Using Olson's (1965) logic of collective action, there are high returns for membership of a group that seeks benefits for a small number of group members and low incentives to join a group that attains benefits for all society. Eising (2007) uses organisational theory to illustrate that business groups are more likely to organise quickly and achieve their preferences than those representing diffuse interests as the benefits are higher for members. Several studies argue that business interest group are more influential than NGOs as they have strong financial resources and supply policy information that creates positive economic incentives for policymakers (Coen, 2007; Dür & de Bièvre 2007; Beyers & Kerremans 2007; Dür & Mateo 2016; Eising, Rasch & Rozbicka 2017)

However, other studies argue that finance does not affect interest group success (Mahoney, 2007; Baumgartner et al. 2010). Dür et al (2015) showed that collective business interest associations are often more successful than private firms in achieving an outcome, even though the firms themselves are richer. Woll (2006) argues that strategies, such as lobbying multiple venues of the EU and focusing on lobbying at the formulation and revision stages of policymaking are important causes of influence. However, studies show that lobbying multiple venues is difficult and wealthy groups inevitably are more successful in overcoming difficulties (Aspinwall and Greenwood 1998; Greenwood, Suddaby & Hinings 2002; McKay, 2012).

McKay (2012) argues that experienced lobbyists are more likely to exert influence. Experience when coupled with wealth will have a positive impact on success. Apollonio & La Raja (2003) agree, arguing that financial capital, membership and experience are important factors. Legislators care about experience and reputation and take it into account when listening to interest groups' potential contributions to the legislative process. Bernhagen and Mitchell (2009) and McKinley and Kroll (2015) discuss the relationships that interest groups forge with government officials and its positive effect on lobbying outcomes.

Turning to non-permanent characteristics of interest groups, Dür & de Bièvre (2007) examine the expertise of interest groups on a specific issue and its effect on influence. Expertise is

circumstantial depending on the issue. An interest group that provides relevant information on an issue will be influential as it alleviates the informational deficit of the EU. Michalowitz (2007) highlights the importance of information as a resource by highlighting two types of influence: technical or directional. Technical influence is comparable to expertise whereas directional influence refers to an interest group's attempt to steer the proposal in another direction. Technical influence has a positive outcome on influence whereas directional produces nuanced results. However, Klüver (2013) deduces that expert knowledge has a positive effect only when it works collectively with other interest groups creating a debate whether interest groups can influence the outcome without the help of other groups.

To summarise the review, the development of interest group theory has allowed researchers to explore new methods of analysing interest group success. Using established theoretical methods has provided justification for certain factors explaining why some groups are more successful than others. However, the review has shown that a debate still exists on what factors best explain interest group success. This creates a gap in the literature where these debated factors are tested through a theoretical framework by combining approaches. This research looks at the implications that these factors have in explaining who is winning in EU digital policy.

3. The EU Institutions

This chapter outlines the three main institutions of the EU and their role in the legislative process. The EU provides several routes for interest groups to have their voices heard in developing European policy (Bouwen, 2002). The three main institutions which provide access to interest groups are the Commission, the Parliament and the Council. It is important to understand the process of making proposals through the ordinary legislative procedure of the EU and the powers that each institutional actor has in developing policy.

3.1 The European Commission

The European Commission has the formal right to initiate the legislative process; as such it is referred to as the agenda-setter. The Commission is divided into governmental departments known as the Directorate-Generals (DGs). The DG responsible for this policy area initially drafts the legislative proposal and requires policy-relevant knowledge to improve the standing of the proposal (Michalowitz, 2002). For this reason, the Commission invites interest groups to

participate in developing policy proposals through public consultations and informal and formal meetings. The Commission is relatively open to the in-put of interest groups as it seeks to ensure its proposals are legitimate, information rich and acceptable for the Council and Parliament (Bouwen, 2002). In order to be granted access to the Commission, interest groups must sign up to the EU Transparency Register which is a database providing a list of pre-approved interest groups that participate in lobbying in Brussels. Once the proposal is created, it is sent to the Parliament and Council to be debated and amended.

3.2 The European Parliament

The European Parliament is a directly elected body of the European Union by the citizens of the member states. It has become an important venue for interest groups to lobby due to its increased power on making legislative decisions (Michalowitz, 2002). The Parliament amendments proposals created by the Commission. The Parliament requires participation from interest groups to reduce its reliance on other institutions for information. Similarly, for the Commission, interest groups provide expert knowledge to Members of the European Parliament (MEPs) which help them in making amendments to policy proposals. However, the information required is less technical than required by the Commission as the proposal is already made (Michalowitz, 2002).

Interest groups target specific MEPs who have been selected for a specialised committee which manages the legislative process of that policy in the parliament. These committees headed up by a ‘‘rapporteur’’, conduct most of the work in amending the proposal on behalf of the parliament. However, all MEPs can vote on accepting or rejecting a proposal. The Commission listens to the Parliament’s amendments and can adjust the proposal accordingly. The other legislative body that can make amendments is the Council.

3.3 The Council of Ministers

The Council represents the member states’ national government interests at European level. The Council meets four times a year where relevant national government ministers meet in Brussels to debate and amend policy proposals which correspond to their national department. Approximately 80% of the work of the Council is conducted by COREPER which a permanent administrative body in Brussels which prepare information for the ministers when they arrive in Brussels to vote (Hix & Hoyland, 2011). Unlike the Commission and Parliament, COREPER

manages its process behind closed doors using a network of national government personnel to make decisions. Therefore, it is not overly receptive to interest group participation at Brussels level (Vidacak, 2003). However, lobbying can take place in other forms through national platforms. Interest groups that successfully lobby national governments can have their interests brought to Brussels by national ministers (Michalowitz, 2002). Occasionally, interest groups can participate with working groups within the Council should circumstances call for it (Greenwood, 2007).

The Council votes using two methods: voting by unanimity which requires all 27 ministers' approval, or qualified majority voting (QMV) (Hix & Hoyland, 2011). The latter is used when Council votes on a proposal created by the Commission. QMV, also known as the "double majority" rule requires 55% of member states representing 65% of the total EU population to reach a qualified majority. As such, not all member states have the same voting power in the Council. Barr and Passarelli (2009) have developed a framework which quantifies the weight that each member state's vote carries in the QMV process.

Similarly, to the Parliament, the Council can accept or amend the Commission's proposals. If the Council and Parliament fail to agree on an accepted proposal an interinstitutional meeting is launched. This conciliation committee is conducted with members from the Commission, Council and Parliament to seek a negotiated outcome to the legislative process and produce an agreed policy outcome (Hix & Hoyland, 2011). This committee meets behind closed doors without public consultation which results in little information being provided on how outcomes are achieved. This poses a difficulty for researchers of EU politics as trialogues have become commonplace in developing EU policy.

Taking the information from chapter 2 and 3 into consideration, the next section will develop important aspects further to create a theoretical framework.

4. Theoretical Framework

The literature illustrates three theoretical approaches in determining influence of interest groups - issue-specific characteristics, interest group characteristics and institutional factors. The conclusions from the literature do not converge on their findings. The hypotheses below are arranged in order to reflect these three schools of thought. Hypotheses two, six and seven refer to

a specific EU institution as it is not anticipated that they will hold true for the other institutions in question whereas the other hypotheses are more general and can be applied to all three institutions.

4.1 Issue specific approach

Issue-specific factors are important elements in explaining an interest group's ability to exert influence on the legislative proposal (Mahoney, 2007). The literature (Mahoney 2007; Kluver, 2011; Michalowitz, 2007) indicates that there are three factors to consider in measuring issue specific characteristics; scope, degree of conflict and salience. As illustrated in the literature review, there is a debate on salience measurement and its effect on lobbying outcome. Therefore, it will be analysed here.

4.1.1. Public salience

As seen in the literature, public salience refers to the amount of attention an issue receives in the legislative process. There are two prominent approaches in measuring salience, Klüver (2011) and Mahoney (2007). Klüver (2011) measures public salience by the amount of attention an issue receives from different interest groups. She argues that it does not have a constant effect on lobbying, rather influence depends on the size of a coalition a particular lobby group belongs to. If an interest group belongs to a large coalition of interest groups, salience will have a positive effect on influencing the outcome. As this research aims to analyse the influence of individual firms rather than a coalition, Klüver's (2011) approach will not be selected.

Mahoney (2007) measures the degree of public salience of an issue by the amount of news coverage it gets. In doing so, she equates salience to the degree of public attention an issue receives. In the case of the EU, she examines the number of Financial Times articles per issue in a two-year period. As public attention increases, so does the scope of the issue where more preferences need to be appeased. Policymakers will not take the viewpoint of one interest group as high salience means the public are watching closely and will scrutinise legislators for appeasing one voice only (Mahoney, 2007). Institutions must appear democratic and fair to remain legitimate to the public. As the salience of an issue is increased, the ability for an interest group to achieve its desire on a policy outcome diminishes. Therefore, following hypothesis is derived:

H1: the more public attention there is on an issue, the less likely an interest group can achieve their desired policy outcome.

4.1.2. Salience at the parliament:

Public attention is an important factor to consider when measuring interest group influence at the parliament as it is directly elected and accountable to the public. As the Council and Commission are not directly elected bodies, this hypothesis is not expected to hold true for them. Michalowitz (2002) demonstrated that the Parliament encourages participation of interest groups. As mentioned in chapter 2, Hix and Hoyland (2011) present arguments for MEPs' allegiance to certain interest groups. In Hix and Hoyland (2011), Stigler's normative argument about the parliament assumes that a politician's main goal is to seek re-election. As the parliament is directly elected by the public, politicians have an incentive to appease voters and support issues that are beneficial to general society. However, as Stigler (2011) argues; "the average voter tends to be rationally ignorant about the details of specific regulatory policy proposals" (p. 191). When issues are not important to voters, politicians can provide beneficial policies to those who have a large stake in that issue, namely private business interests. Business organisations have an abundance of resources that supply politicians with financial resources and information on voters which are used to fund election campaigns (Hix & Hoyland, 2011). When the media is not actively monitoring an issue, politicians are free to appease business interests without fear of backlash from their voters. This research argues that public salience is a pre-condition for how parliament is likely to vote on an issue.

H2: In issues of high salience to the public, the parliament is likely to support public interests to appease their voters.

H2.1: However, in issues of low public salience, the parliament is more likely to satisfy business interests as they are not being scrutinised by the public.

4.2 Interest group characteristics approach:

As illustrated in Chapter 2, interest group characteristics can be permanent or non-permanent and used to explain why some groups are more successful than others in achieving policy preferences. The following section looks at different factors with respect to business associations and NGOs active in shaping EU digital policy.

4.2.1. Interest group type

Interest group type is an important characteristic and can affect a group's ability to influence a policy outcome (Olson, 1965; Coen, 1997 Dür & de Bièvre, 2007). Olson (1965) and Hix & Hoyland (2011) demonstrate that there are high incentives to join a group that seeks benefits for the members of their group only and low incentives to join groups that seek benefits for all of society. This suggests that private interests have greater incentives to lobby than NGOs. This is due to the "free-rider" problem that can occur with organisations representing diffuse interests i.e. NGOs. Olson (1965) argues that with respect to diffuse groups, their incentive to supply resources to lobby decreases as they will not enjoy a better outcome than anyone else in society. The benefit of their desired outcome is non-excludable thus creating an incentive for groups to "free-ride". Private interests seek benefit for their members only and therefore have greater incentive to lobby as the potential return is higher. Therefore, a private interest group is more likely to achieve their desired outcome.

However, this is not always the case. Mahoney (2007) illustrates that when public opinion is high on an issue, it raises public scrutiny on lawmakers. This is an important factor to consider and can change the behaviour of the policymaker vis-a-vis interest groups. Policymakers do not want to appear to favour one group over another so will listen to input from a multitude of actors. As theorised above, the parliament is expected to be sensitive to salience. However, the Council and Commission are also subject to media attention. The EU has an incentive to get its legislation passed and appear legitimate, fair and democratic. It is a body for the betterment of EU citizens (Hix & Hoyland, 2011). Therefore, if public opinion is focused on an issue, the institutions are more likely to listen to those representing public interests.

H3: Business associations will be more likely to achieve their desired policy outcome compared to NGOs.

H3.1: However, interest groups lobbying for diffuse goods are more likely to be successful in achieving their desired outcome on a highly salient issue compared to those advocating for private interests.

4.2.2. Finance

As illustrated in chapter 2, there is a debate on the effect finance has on an interest group's ability to achieve its outcome. Eising (2007), a strong proponent of the theory, argues that the most successful interest groups are the ones that have strong financial means and supply legislator's information that yields economic incentive. Dür & de Bièvre (2007) argue that private interests are strong at attaining their desires in policy outcomes due to their financial wealth. They can devote more resources to activities which produce a positive outcome. Wealthy groups can lobby multiple venues of the EU and hire more staff to arrange conferences promoting their cause and engage with media to enhance their position.

H4: The wealthier organisation will be more influential in obtaining their desired outcome.

4.2.3. Established relationships

McKay (2012) looks at personal rapports between interest group staff and institutional staff as an indicator of lobbying success. Relationships are built through frequent meetings and experience. Through relationship building with EU personnel, interest groups can develop meaningful insightful strategies and improve their ability in achieving their desired outcome (McKinley & Kroll, 2015). It is usually wealthy private firms that achieve this as they can pay higher salaries and attract experienced lobbyists who have good reputations and prior contact with EU personnel (McKay, 2012). McKinley and Kroll (2015) argue that lobbyists compete for access to lawmakers. According to this study, "lawmakers have an incentive to provide greater access to citizen-donors and lobbyists with whom they have a relationship" (see III. Conclusion). As Bouwen (2002) illustrates, access to lawmakers is a likely indicator of influence. Therefore, groups with an established relationship with EU personnel are likely to be successful.

H5: The stronger the relationship is between the lobbyists and institution staff members; the more successful lobby groups will be in achieving their desired outcome.

4.3. Institutional approach

Bouwen's (2002) study illustrates that the characteristics of EU institutions matter in explaining why some interest groups gain access better than others, increasing their chances to achieve their preferences. Whilst this chapter has already derived a hypothesis for the parliament, this section looks at who is likely to be successful at the Council and Parliament.

4.3.1. Interest groups at the Council

As illustrated in chapters 2 and 3, the Council provides fewer opportunities in Brussels for interest groups. However, Michalowitz (2002) argues lobbying success is possible for interest groups that lobby national governments. An interest group with an established presence in a member state capital is more likely to have access to decision-makers in that member state's government (Bouwen, 2002). By influencing a national government decision, this in turn will influence their decision at Council. Some interest groups have several offices spread across the union which increases their ability to access multiple national governments.

Many interest groups are solely Brussels based whereas others are more international, with regional offices or membership representation in Europe. From this, one can deduce that interest groups with multiple representations are more likely to be successful at Council. The Shapley-Shubik scale, outlined in Chapter 3, illustrates that some countries have greater voting power at the Council and therefore more beneficial to interest groups (Barr and Passarelli, 2009). Taking these elements into account, the following hypothesis is formed:

H6: Interest groups with greater lobbying activity in the member state's capitals are more likely to be influential at the Council than interest groups that are Brussels based only.

4.3.2. Interest groups at the Commission

Bouwen (2002) argues that the Commission seeks participation from interest groups for several reasons. As the agenda setters of the legislative process, the Commission needs expert knowledge on a topic from relevant interest groups to improve their proposal. As the Commission's administrative bureau is relatively small, it requires interest groups to supply information and reduce the knowledge deficit it faces in creating proposals (Bouwen, 2002). Whilst the Parliament and Council also require expert knowledge, their reliance for this is smaller than the Commission as the legislative proposal has already been created (Bouwen, 2002).

Expert knowledge is circumstantial and can change depending on the policy issue in question (Michowlitz, 2007; Mahoney, 2007; Dür & de Bièvre, 2007). Therefore, expert knowledge is a non-permanent resource supplied by the interest group. Although the Commission has the sole right to initiate legislation, it suffers from a knowledge deficit due to an understaffed

bureaucracy unable to provide substantial knowledge in creating policy (Hix & Hoyland, 2011; Michalowitz, 2007). The Commission requires the input from interest groups that are resource rich on a required topic, i.e. digital affairs. Michalowitz (2007) argues that a group that provides the most relevant technical expertise without trying to change the direction of the policy is likely to be influential. The business associations who specialise in an area of the policy being created are likely to be attractive to the Commission due to their abundance of resources and expertise on the matter. In this case, interest groups representing technology infrastructure are likely to be successful.

H7: The interest group who can supply the most appropriate policy-relevant information to the Commission is most likely to achieve their desires with the Commission.

The hypotheses will be analysed with respect to EU digital policy to provide an answer to the research question. It is expected to the hypotheses will illustrate what groups are winning and what theoretical factors best explain interest group influence with respect to this case.

5. Research design and methods

This chapter discusses available research designs and methodologies arriving at the most suitable option in answering the research question. It discusses the methodology and units of data used including interest group, case selection and data sources. The following section presents a review of available designs arriving at the most appropriate method.

5.1 Quantitative cross-sectional design

Scholarly literature exists on the availability of observational and experimental research. Due to the scope and resources available for this research, it has already been decided to focus on an observational study rather than experimental. Two types of observational studies have been highlighted: time-series and cross-sectional. Time-series observational studies focus on a time stamp over several time periods to illustrate variation (Hudson, Fielding & Ramsey 2019). This research is not concerned with examining the change of influence of interest groups over a long period of time. This research focuses on recent lobbying efforts through the latest developments of EU digital policy. Therefore time-series design has not been chosen for this research.

Blatter and Haverland (2012) define cross-sectional design as a methodological approach that "presents empirical evidence of the existence of co-variation between an independent variable X

and a dependent variable Y to infer causality" (p.33). The cross-sectional design when conducted as a large-N study can strengthen the application of the research to multiple cases and support theoretical generalisation (Gschwend & Schimmelfennig, 2007). However, it does not explain one case in detail, therefore not illustrating specific features that can be unique to policy areas. This research aims to investigate factors of influence in EU digital policy, so a quantitative study has not been chosen. However, this design has several strengths for this research. First, the researcher must select controlled independent variables and conduct a regression analysis on the data gathered through research to give a result. This research aims to demonstrate a relationship between the chosen independent variables and the dependent variable of influence. Second, this method is popular due to its ability to control for confounding variables, which is where a variable can influence both the dependent and independent variables.

In order to use this approach, the number of cases would need to be increased. The units of analysis for this research are digital policies and the business associations and NGOs who lobby on these policies. As this research is concerned with NGOs and business associations who extensively lobby on digital policy, this reduces number of observed cases to fall below 25 (small-N). There are other groups and private citizens who lobby EU institutions, but their lobbying efforts are minimal compared to the larger groups chosen for this study and their effect on the outcome is negligible (Atikcan & Chalmers, 2019). This study could increase the scope to include other private firms but business associations represent these interests. Industries such, big-tech, finance and telecommunications are particularly interesting due to their vast size and commitment to lobbying digital policy (Newman, 2010; Atikcan & Chalmers, 2019). In order to limit the scope of the research, business associations representing these industries are selected. Therefore, a qualitative (small-N) design will be applied.

5.2 Case study

A case study is a small-N, in-depth analysis of a single unit which allows for detailed research compared to other, quantitative, designs (Blatter & Haverland, 2012). It has several advantages as initially "[c]ase study researchers can, ceteris paribus, reflect more intensively on the indicators they use to score the cases" (Blatter & Haverland, 2012; p. 64). Second, case studies are useful approaches when looking for answers in a policy field as "small-N research typically outperforms large-N research in terms of the concept validity of measurement" (p.64). The study

of a single case or many cases allows the researcher to select indicators that are contextually relevant to that specific case (Blatter & Haverland, 2012). However, it should be noted that these indicators may not be generalised and their application to other cases may not be possible. Case studies are useful for examining specific policy areas and their unique characteristics. As this research aims to illustrate the important factors in explaining success of interest groups through digital policy, it is an appropriate design. Within case studies, there are two approaches: co-variation and congruence. Co-variation (COV) design compares at least one case and looks for co-variation between them whereas congruence (CON) tries to establish congruence between theoretical expectations and observations from empirical evidence in the chosen case (Blatter & Haverland, 2012).

CON can be used when the researcher is looking at empirical evidence to explain why one theoretical approach is stronger in explaining an outcome compared to another theoretical approach (Blatter & Haverland, 2014). For this research to be conducted as a CON approach, issue characteristics, interest group characteristics and institutional factors would be used conclude which theoretical approach is strongest. However, this research is interested in examining specific factors that explain the outcome of digital policy rather than examining which theoretical approach is stronger. Furthermore, theoretical approaches have been combined in the theoretical framework. Therefore, CON is not a suitable approach for this research. COV attempts to analyse whether a set of independent variables (X) which vary greatly relative to each other cause an outcome on the dependent variable (Y) (Blatter & Haverland, 2012). As this research looks at what elements from issue-specific characteristics, interest group characteristics and institutional factors (X) explain what groups are succeeding in EU digital policy (Y) it is an appropriate design.

5.3 Validity and reliability

It is important that research accounts for validity and reliability. Validity refers to the use of correct indicators and variables in a study. In his evaluation of validity, Mitchell (1985) discusses internal validity whereby "[s]pecific attention needs to be paid to data selection to ensure validity of this COV research. Internal validity deals with the question of whether the experimental treatment (variable A) did indeed have an effect (on variable B)." (p. 193). When there is a lack of internal validity in a case, there can be an alternative argument made on the effect of the

independent variable on the dependent variable. The dependent variables are chosen factors that express what we want to prove from theoretical discussion. These are then operationalised through analysis (Mitchell, 1985). To ensure validity of this research, the variables are derived from academic literature outlined in chapter 2, 3 and 4. The indicators assigned to these variables are the same methods used in previous research. In some cases, an alternative variable was used due to the lack of data available for this research. For example, in measuring relationships between interest groups and lawmakers McKay examines the personal rapports between a lawmaker and an experienced lobbyist. Due to data protection rules and the inability to conduct interviews, an alternative measure was chosen of Commission meetings. Whilst it is not the most accurate measurement reflected in literature, the meetings are officially recorded and indicate personal interaction between interest group staff and lawmakers inside the Commission.

It is difficult to establish a time sequence of events and thus identify the causal path of the observed variables (De Vaus, 2001). In other words, does X lead to Y or vice-versa. One way of overcoming this is through the literature review. In this case, the literature demonstrates that various characteristics of interest groups and issues cause influence. This is sufficient in ruling out reverse causality. The literature review elaborates on theory and empirical knowledge which helps the researcher in selecting the most suitable independent variables which determine the causal relationship between X and Y (De Vaus, 2001).

Reliability refers to the trustworthiness of results. To ensure reliability of the design, Riege (2003) suggests “use of multiple sources of evidence in the data collection phase” (p. 82). Mitchell (1985) also recommends using data sources that pre-date the event being tested. In order to improve the reliability of this research, a triangulation of documents, position papers, EU official papers, newspaper articles, official blog posts and public consultation posts will be used. Most of these documents were written before the outcome of the directives which improves validity (Mitchell, 1985). Supplementary documents in which interest groups evaluate the directives after they were enacted are sometimes used as to clarify a group’s position or if no other documents were found. Position papers are strong data sources to ensure reliability of the research compared to interviews. If the research was repeated using position papers, the outcome would be the same. However, interviewees could provide an alternative response which alters the outcome of the research.

5.4 Case selection

The section discusses the criteria for choosing cases and interest groups for this research.

In order to test the effect of salience two case studies have been chosen: one salient and one non-salient case. In order to be selected, the case studies must meet certain criteria. According to Blatter and Haverland (2012), the cases should be controlled with similarity between all variables except the independent variable which should differ greatly, in this case salience. Initially, proposals that were subject to EP hearings and public consultations by the Commission post-2010 were chosen. There is limited research conducted on these cases and they call for an in-depth analysis. The EU has ramped up on digital policy proposals in the last ten years and many digital NGOs and business associations have registered on the *EU Transparency Register* within the last ten years (Cooper & Hirst, 2017).

Second, the directive/regulation must be open to participation of interest groups, which is confirmed by public consultations held on the issues. This provides data for the researcher. Following this consultation, the Commission should draft a legislative proposal on the issues raised. Third, there should be strong variance between high and low public salience between the issues. Fourth, as this study investigates NGOs and business associations' ability to assert influence under conditions of high and low salience, two case studies are selected that were lobbied extensively by multiple interest groups. Lobbyfacts.eu and the public consultation list were consulted to ensure that enough interest groups lobbied on both issues. Finally, this research is interested in EU digital policy, therefore issues concerning the digital single market were chosen.

From these criteria, the NIS directive (EU 2016/1148) and the GDPR (EU 2016/679) have been highlighted as suitable options. In order to confirm the degree of salience of the cases, both were analysed against the Financial Times database. This study uses Mahoney's (2007) method to assess the degree of salience of an issue to the public selecting the Financial Times as a credible source of European affairs. For this research, the timeframe between public consultation and the final Parliament vote was used. The researcher manually coded the articles as to whether they explicitly refer to the chosen directive or not. If there was ambiguity on whether articles referred to the policy proposal in question, they were omitted from the search. The results illustrate 51

articles for the GDPR and 3 for the NIS Directive. This demonstrates a strong variance in the issues selected and therefore both cases are applicable for this research.

5.5 Interest Group Selection

Interest groups need to meet specific criteria to be selected for this research. There needs to be suitable control and variability between the two sets of interest groups to test the hypotheses outlined in chapter 4 (Blatter & Haverland, 2012). This assures variation between independent variables which can be used to examine alternative explanations to the outcome. (Bunea, 2013). Initially, interest groups were selected from two broad categories: business associations and NGOs representing public interests. This assures variation in group type and financial resources as NGOs are usually less well-endowed than private firms. Second, there must be a divergence in preferences between the groups, only NGOs representing public interests and business associations lobbing for sector-specific interests were chosen as they lobby for different outcomes in EU legislation (Coen, 1997; Eising 2007). Third, interest groups must have actively lobbied on the cases in either directly through public consultations or by producing public position papers.

Private firms were omitted due to the lack of data available on their lobbying practices when these proposals were launched. Furthermore, the use of industry specific business associations gives a holistic overview of the influence of that industry. Think tanks, educational institutes and public authorities have also been left out of this study to limit the scope as the criteria for measuring the hypotheses can be satisfied without analysing them. Single-issue groups such as National AIDS Trust were also omitted as they did not provide enough preferences to be measured for this study.

To confirm the selection of the interest groups, they were analysed on the *EU transparency register*. NGO categorised as *III - Non-governmental organisations* on the register were chosen ensuring that the NGOs represent public interests (Europa L277/11, 2014). Business associations which represent with a stake in the digital economy have been chosen for this study. Atikcan & Chalmers (2019) demonstrate from their research that big-tech and financial institutions stand to gain and lose the most from EU digital legislation due to their economic reliance on the industry. Groups representing telecommunications industry and aviation industry were also chosen as they participated heavily in the consultation phase of legislation. All business associations in this

study are registered as *II - In-house lobbyists and trade/business/professional associations* on the register.

The following tables 1 and 2 provide the names of the interest groups that have been chosen for this study.

Table 1: Interest groups chosen for salient directive (GDPR)

Interest group name	Acronym	Type
European Digital Rights Initiative	EDRi	NGO
The European consumer voice in standardization	ANEC	NGO
Access Now	AN	NGO
Verbraucherzentrale Bundesverband (Federation of German Consumer Organisations)	VZBV	NGO
DigitalEurope	DE	Business Assn.
American Chamber of Commerce in Europe	AC	Business Assn.
European Banking Federation	EBF	Business Assn.
Global System for Mobile Communications	GSMA	Business Assn.

Table 2: Interest groups chosen for non-salient directive (NIS)

Interest Group name	Acronym	Type
European Digital Rights Initiative	EDRi	NGO
Bits of Freedom	BoF	NGO
Access Now	AN	NGO

EURid Domain Registry	EURid	NGO
DigitalEurope	DE	Business Assn.
American Chamber of Commerce in Europe	AC	Business Assn.
European Banking Federation	EBF	Business Assn.
European Cockpit Association	ECA	Business Assn.

5.5. Measuring Influence: Methods Available:

This section outlines three established approaches in measuring influence; process-tracing, attributed influence and preference attainment, their strengths and weaknesses in measuring influence as proposed by Dür (2008). The research arrives at a justification for choosing preference attainment for this research.

5.5.1. Process-tracing

This approach attempts to illustrate the intervening causal process and establish a causal chain between independent variables and the outcome or on the dependent variables (Dür, 2008). It is a step by step process where researchers attempt to identify the causes that affect the outcomes. Within the EU, it is one of the most used approaches in qualitative small-N research in measuring interest group influence. Researchers record a range of factors including interest group preferences, their attempts to influence the policy, their access to decision-makers, the response from decision-makers and surveys with interest groups to measure their satisfaction or dissatisfaction with the final outcome (Dür, 2008). It is a useful process to determine the influence of a single group.

Dür discusses two strengths in using this process. In qualitative research, if the researcher has good knowledge on most factors influencing a political decision, it allows them to discuss alternative explanations on a policy outcome before concluding whether or not the examined interest group had an independent effect on the policy outcome (Dür, 2008). Semi-structured interviews are used in this method which gives the researcher to obtain information from the interest group that they may not have been able to acquire otherwise.

There are disadvantages to using this approach. Firstly, it can be difficult to obtain the empirical evidence necessary for process-tracing. Even if all steps on the causal chain are identified, data is not always available to fill these gaps. This can lead to a false result if the researcher concludes there was no influence from a specific interest group because a piece of data could not be found (Dür, 2008). Lobbying often takes place in secret, and many interest groups are reluctant to divulge sensitive data (Dür, 2008). Another issue with this method lies with the over-reliance on interviewees for data. This data is not always reliable as interviewees do not always represent a situation accurately. Information given from interviewees should be cross-checked, but this is not always possible. As no interest group was available for interview for this research, process-tracing has not been selected in measuring influence.

5.5.2. Attributed influence

This method of measuring influences relies on surveys where interest groups are asked to assess their own influence and their peers. Third parties who report on interest group influence can also take part (Dür, 2008). This is an advantageous method as it's relatively easy to conduct. This method has a wide scope as it usually accounts for all channels of influence (direct lobbying, outside lobbying, selection of decision-makers and structural power) as discussed by Dür (2008). However, there are disadvantages to using this method. Asking interest groups to self-assess can lead to a bias in results if they under or overestimate their ability to influence an outcome. Furthermore, this method does not measure actual influence, but perceived influence of an interest group on an outcome. Finally, surveys can be disadvantageous as they can lack detailed information such as the type of influence exerted by the interest group. As interest groups were unavailable for participation in this study, the attributed influence method was not chosen.

5.5.3. Preference Attainment

A third method proposed by Dur measures interest group influence by analysing the group's degree of preference attainment in the policy outcome (Dür, 2008). This method matches the outcomes of the legislative process with the preferences of the interest group. The distance between the outcome of the policy and the desired outcome of the interest group illustrates the influence of that group. Researchers attempt to control other variables which explain why the outcome can move closer and further away from the group's preference (Dür, 2008). It is argued that increasing the number of issues or cases analysed reduces the error in this research.

There are several advantages to measuring preference attainment. Initially it can illustrate success of an interest group even if there are no visible reasons for this. It is important to remember that much lobbying happens in secret and data is not available to explain how a group attained their desired outcome (Dür, 2008). It is more likely to show influence compared to process-tracing. Secondly, preference attainment when successfully applied to large-N research allows for a generalisation of findings.

There are disadvantages to this method. Initially, it can be difficult to determine preferences of actors. Position papers focus on certain issues and omit other preferences, sometimes on purpose. However, the industry in which that actor operates can give clues of their preferences e.g. agricultural producers generally favour trade liberalisation (Dür, 2008). Second, it is difficult to rule out alternative factors which explain the influence of an interest group on the policy outcome. Mahoney (2007) argues that a random selection of cases cancels out alternative explanations for outcomes. However, excluding different explanations is difficult. Finally, this method can lack attention to detail as preference attainment does not necessarily illustrate what channel of influence was used (Dür, 2008).

This study focuses on understanding on whether interest groups are successful in achieving their preferences and what variables explain this success. Therefore, preference attainment is an appropriate method and will be chosen for this study.

5.6. Method chosen for study

Dür (2008) reminds researchers that the three measurements have their strengths and shortcomings. In order to strengthen the research, this study will use preference attainment method using multiple sources of data to reduce error. Vannoni and Dur (2017) argue that for small-N studies, preference attainment should be supported with various data sources including interviews or multiple documents. Process-tracing and attributed influence have not been chosen as they require active participation of interest groups in the research which was not possible due to the busy schedule of interest groups.

Preference attainment presents itself as a suitable option for several reasons. First, preference attainment can answer the research question indicating what variables explain interest group success. Second, sufficient data is available to conduct the preference attainment method.

Although interview data is unavailable, documents and archives provide supplementary sources. Third, the application of this method for small-N research adds to the theoretical discussion on new ways to measure influence.

A combination of Bunea's (2013) and Mahoney's (2007) methods of measuring preference attainment has been chosen. Mahoney (2007) examines an interest groups preference on multiple cases rather than a specific case (large-N). In order to examine preferences of interest groups on a single case, it has been adapted to incorporate elements of Bunea's (2013) method in establishing key issues of that case to measure multiple preferences of interest groups on one case. By measuring multiple preferences of issues in a single case, it increases the reliability of results and provides in-depth insights on EU digital policy. It is important to mention why Bunea's (2013) method was not chosen in isolation. Bunea (2013) evaluates environmental policy where she establishes a status quo preference using previous environmental legislation as a benchmark. This is not possible for digital policy where preferences are more nuanced. Furthermore the status quo is not always easily established in digital policy as it is a relatively new phenomenon, especially cyber security.

5.7. Operationalisation

Initially, responses the public consultation documents submitted to the Commission are coded to highlight preferences of actors. The content is disaggregated into the core issues of importance for the groups involved. As a plethora of issues are raised at this stage, it is important to focus on the most important issues to narrow the scope. When multiple interest groups discuss the same issue or provide detailed information it is considered important (Bunea, 2013). If an issue is raised by one interest group that is unlikely to be met with any opposition from other groups it is not important, and therefore omitted. Eight issues per case, sixteen in total, were established. The issues are clear, related to the subject of the consultation, divergent from one another, and subject to opinion by most interest groups under research.

Once the issues are defined, the preferences of the actors on these issues are established. Mahoney (2007) coded for lobbying success by considering their objectives on a campaign. Data sources are used to highlight the preferences of the business associations and NGOs according to the issues chosen for this case. These preferences will be matched against the preference of the Commission, the Council, the Parliament and the final legislation to understand what interest

groups are succeeding and where. Official EU documents illustrating the position of each institution are used.

As illustrated in the literature review, lobbying is not a zero-sum game. Interest groups are likely to achieve some of their preferences and forgo others. Mahoney (2007) accounts for this by measuring the degree of lobbying success of an interest group per case. This is adapted to measure the degree of lobbying success per issue in the case. Each group is graded on how well they did at achieving their preferences. For each issue, an interest groups preference will be matched to the outcome at each institution. Below in table 3 a summary of how preferences are graded:

Table 3: Grading of preferences

Score	Explanation
0	Interest group attained none of their preferences on an issue
1	Interest group attained some portion of their preferences on an issue
2	Interest group attained all preferences on that issue

Own illustration, content adapted from Mahoney (2007)

As eight issues are measured, a group that achieves all their preferences scores 16, (8 x 2) = 16. Not all groups provide a preference on all issues. If an interest group provides seven preferences, their total score is out of 14. As this research is illustrating to what extent interest groups are achieving their desired outcomes rather than their ability to shape the outcome of the proposal it is an applicable method to use.

The next section discusses the type of data used to find and measure preferences and how this approach improves the reliability of results.

5.8. Data Collection

According to Yin (2009), there are six resources available which are primarily used in case studies. These include documents, interviews, archival records, physical artefacts, direct

observation and participant-observation. Yin (2009) recommends a combination of these sources as all have their strengths and weaknesses. For this study, a combination of documents and archived files are used. The other sources are not relevant for this type of research and have been omitted. The following section discusses Yin's (2009) recommendations and the types of documents used.

Yin (2009) discusses various document sources which can be considered when conducting research. Administrative documents, newspaper articles, official meeting notes, academic studies and internal record documents are examples of such. Multiple documents should be used consecutively to corroborate and augment evidence from multiple sources (Yin, 2009) In order to identify the preferences of the interest groups for this research a combination of official position papers, public statements, blog posts representing the interest groups' view and answers to public consultation surveys will be considered. Although a combination of sources will be used, there is still a chance of a biased result. Written documents have been written for specific purposes rather than this research and may contain data which is meant to be interpreted in a different way (Yin, 2009). Blogs can suffer from a reporting bias in that it can misinterpret events, suppress information and emphasise miniscule events with the aim of enhancing their own viewpoint (Yin, 2009). It is advised the researcher to triangulate the data from other sources to enhance the evidence and improve results (Yin, 2009) This research is aware of these limitations and does not rely heavily on a singular document when analysing the preference of a group on a phenomenon.

5.9. Overcoming obstacles with desk research

There were several challenges in finding data to complete this research. This process should be highlighted with future research on EU digital policy. Due to a change in policy by the Commission, public consultation documents pre-2017 are no longer publicly accessible online. Therefore, it was decided to use alternative methods in retrieving public consultation documents and use data sources as supplementary tools. Initially, representatives from DG CONNECT and DG JUSTICE were contacted for access to the documents. This proved useful in finding institutional information about GDPR and NIS which was incorporated into the analysis. Second, several Boolean strings were constructed to find position papers on these cases. From this several documents were sourced online. Third, several interest groups were contacted by email with respect to arranging interviews and gathering documents. Employees who worked for the

organisation during the time of the legislative process were also contacted on LinkedIn. Reputable media outlets also proved fruitful in establishing leads on the main actors involved. Unfortunately, many links had been removed due to the time-lapse in which this legislative happened.

As this data was not sufficient, the research investigated digital archive portals to retrieve the data. Locatelli (2017) provides a guide in how to use digital archives to source data for academic purposes that is accurate, legal, and ethical. Archives that store private intranet networks or store personal data were excluded. This is an important exercise in using digital archives as "[i]n this way, data are not collected if they are protected in a way that is designed to prevent public access" (p.2; Locatelli, 2017). The remaining public consultation responses and position papers for both the GDPR and NIS directive were found through archives, most notably *"Wayback Machine"*.

In interpreting the documents, specific attention was paid to the year of publication. If a group expressed satisfaction in achieving a preference in the initial Commission proposal, it was checked against the final directive to clarify if the group had been successful. In this case, the group would score high on achieving their preference at the Commission but score poorly against the final directive if their preference was not met. Furthermore, interest groups often reflect positively on the outcome of a directive even if they were initially against it. Care needs to be taken in interpreting what interest groups mean when writing proposals.

5.10. Assigning indicators to variables

Following the criteria set out in *4.4 Interest group selection* indicators were assigned to each variable to test the theoretical framework. Each indicator listed is table 4 corresponds to a variable being tested in each hypothesis. The indicators used are the same as the indicators used in the academic literature. Where it was not possible to use the same indicator, alternative measurements were used to improve validity of research. As mention in section 5.3, Commission meetings were used the best alternative substitute indicator. Data is collected from *lobbyfacts.eu* and *EU Transparency Register*. An average figure across six-year span, from 2010 to 2016 was taken as an average measurement for both directives. The tables presented in Annex I provide the data correlating to the interest groups which is used in Chapter 8 to evaluate the hypotheses.

Table 4: Assigning indicators to variables

Variable	Hypothesis	Indicator
Interest group type	H3 & H3.1	Group advocating for public or private good as described on the EU Transparency Register. Derived from Olson's (1965) theory.
Finance	H4	Average annual lobbying budget of interest groups (Coen, 1997)
Relationship	H5	Average number of meetings between interest group and the Commission.
Lobbying in member state capital	H6	Ability to access national government in member states (Bouwen, 2002; Michalowitz, 2002). This includes groups with permanent staff in member state capitals and membership organisations that represent national bureau interests in Brussels e.g. EBF.
Policy-relevant information	H7	Expert knowledge provided by interest group derived from Bouwen (2002) and Michalowitz (2007). Information found on group's website.

Own illustration

To summarise, this chapter has provided justification for the chosen research design and data used to affectively analyse the case and provide reliable and valid results. The next section applies this methodology to the cases of the GDPR and the NIS Directive.

6. Case Description

The following chapter introduces both the GDPR and the NIS Directive. It provides an explanation behind the key issues of each case used for analysis.

6.1 Background to salient case - GDPR

Data protection is an issue which has received much attention from the EU. In 1995, the EU adopted Directive 95/46/EC which provided a regulatory framework on how to manage personal

data flows across the member states (European Union, 95/46/EC). The directive outlined basic principles for data protection which the member states were instructed to write into law. In 2000, the right to personal data protection was enshrined in Article 8 of the *"The Charter of the Fundamental Rights of the European Union "* which states that "[e]veryone has the right to the protection of personal data concerning him or her" (Art. 8, European Union, 2000). By 2003, it was clear that digital advancements were accelerating since the introduction of the data protection directive which resulted in the Commission to consult with governments and interest groups on how to improve the directive to be more adaptable to current technology and future innovations. However, these consultations did not result in any concrete action with the Commission opting to create a more detailed, stricter policy at EU level (European Commission, 2010). In June 2009, the Commission launched a public consultation on data protection inviting stakeholders to contribute to the future of data protection policy in the European Union. The objective of the Commission was to improve the legal framework to make it more adaptable to newer global technologies, strengthen data protection rights for the user and provide clear guidelines to data processors on legal practices regarding processing personal data (European Commission, 2014)

The consultation received 168 responses in total from interest groups. The issues raised by interest groups about data protection and an explanation of what they entail are outlined below.

6.2 Issues of GDPR

Table 5 shows how GDPR has been disaggregated into core issues using Bunea's (2013) method outlined in section 5.7. Issues were derived using public consultation document supported by position papers and other relevant documents.

Table 5: Disaggregated issues for GDPR

1. Consent
Defining what constitutes consent. What signals can be used to clarify consent and what data is subjected to consent.
2. Rules pertaining to processing data

This discusses the main principles on how to process data. It suggests type of data that can collect and the obligation of processors and controllers.
3. Personal Data
Defines what constitutes personal data in a digital age. Discusses the rights of the user and the storage of personal data.
4. Data Breaches
Provides clarification on what data breach notification requirements. Puts a scope on the type of breaches to be reported.
5. Main establishment
For a group of undertakings within the EU, there was an issue on what national authority they would be subject to
6. International Data Transfer
This refers to handling data flows between the EU and third countries and organisations.
7. Privacy by design
This refers to whether security protocols should be included for products and services to comply with data protection measures.
8. Sanctions
How the regulation should be enforced.

6.3. Background to non-salient case - NIS Directive

Cyber security has been an issue at EU level since 2004 with the formation of the European Union Agency for Cyber security (ENISA) under regulation 460/2004/EU. Since then, a series of policies has strengthened ENISA resulting in a transfer of more competencies to this bureau e.g. 526/2013/EU. Although ENISA focuses cyber security, this issue largely remained with the member states. The NIS directive is the first piece of EU-wide legislation on cyber security. The aim was to provide a cross-border approach to improve the overall level of cyber security in the EU. In a EUROBAROMETER survey in 2012, 38% of EU citizens said that they were concerned about online security issues with 18% reporting it deterred them from engaging in

online economic activity. (Euractiv, 2012). The member states have reacted to cyber security by introducing various measures to enhance their digital systems. Before the introduction of the directive, many had introduced strong cyber security measures, causing fragmentation and un-coordination between the member states (European Commission, 2013). The goal of this directive aimed to harmonise approaches and bring cyber security to the same level of development in all EU member states. This would entail improving the security of the internet and the private networks and information systems which run essential services in our society and economy (European Commission, 2013).

Annex II illustrates the key events in the lead up to the NIS directive. In 2012, the Commission engaged with a series of stakeholders. They launched a public consultation on "Improving NIS in the EU" from 23 July to 15 October 2012. 169 responses were received online and another 10 written responses came from the Commission.

6.4. Issues of NIS

Table 6 shows how the NIS policy proposal has been disaggregated into core issues using Bunea's (2013) process, the same as the GDPR.

Table 6: Disaggregated issues for NIS

1. Scope
This refers to the industries which are implicated by the proposed directive.
2. Member State Cyber security Bureaus (EU Security network)
Rules relating to establishing a national cyber security bureau in every member state.
3. Type of Incidents to be reported
This refers to the type of incidents that should be reported under the scope of this directive.
4. Accountability of operators of essential services
This issue refers to whom operators of essential services should be accountable to. This refers to reporting incidents to national authorities or the public.
5. Direction of cyber security
This refers to the guidelines that the EU creates in relation to cyber security. These guidelines

could be in line with existing standards or new European standards.
6. Penalties
How the directive can be enforced by member states and whether this should be an EU competence.
7. Actions to be taken by operators
This refers to the upgrades existing processes and products need to be compliant with this directive.
8. Risk assessment
How firms can demonstrate their compliance and who should be involved in this process.

7. Analysis

The following chapter analyses preference attainment achieved by interest groups on the main issues at the three main EU institutions and the final directive. This data has been derived from own research which can be found in Annex III. Table 7 and 8 present the degree of preferences achieved by interest groups scored out of 16 taken from Mahoney (2007). The results are also expressed in percentage format. The rest of the chapter summarises the findings from the analysis illustrating key findings and trends in both cases.

7.1 Summary of results in the salient case (GDPR)

Table 7: Results of GDPR – salient directive

Interest Group	Group type	Outcome Commission	Outcome Parliament	Outcome Council	Outcome of Regulation
EDRi	NGO	10/16 (63%)	10/16 (63%)	5/16 (32%)	8/16 (50%)
ANEC	NGO	8/14 (57%)	8/14 (57%)	5/14 (36%)	8/14 (57%)
VZBV	NGO	7/14 (50%)	8/14 (57%)	6/14 (43%)	6/14 (43%)
AN	NGO	11/16 (69%)	12/16 (75%)	7/16 (44%)	7/16 (44%)

DE	BA	7/16 (44%)	8/16 (50%)	14/16 (88%)	10/16 (63%)
AC	BA	8/16 (50%)	8/16 (50%)	11/16 (69%)	11/16 (69%)
EBF	BA	4/16 (25%)	7/16 (44%)	10/16 (63%)	10/16 (63%)
GSMA	BA	6/16 (38%)	6/16 (38%)	9/16 (56%)	8/16 (50%)

Own illustration

As shown in table 7 most NGOs and business interests achieved at least 50% of their preferences in the final proposal. As this regulation was large comprising of 99 articles, groups often had their preferences met without causing conflict with other groups. Business associations performed slightly better securing 62% of preferences on average. table 7 suggests that NGOs performed well at the Commission and Parliament whilst business interests performed better at the Council. Therefore, NGOs were satisfied with the initial proposal but less successful with outcome of the final regulation. Conversely, business associations had a poor outcome in the Commission's proposal but increased their position in the final regulation due to legislative amendments. DE and EDRi provide a suitable example. Whilst DE scored 44% at the Commission, the high score of 88% at the Council allowed DE to improve its final position of 63%. Compare this to the large NGO EDRi, who initially scored 63% of their preferences after the Commission's initial proposal but had this reduced to 50% in the final text due to a weak attainment of preferences at the Council of 32% (Table 7). This illustrates that legislative amendments matter.

7.2. NGO preferences in the salient case (GDPR)

This section analyses NGO preferences on issues outlined in table 5 and their success at the three institutions. Compared to business associations, the NGOs analysed in this study converged on many preferences. In general, they advocated on strengthening data protection principles in line with human rights and public interest. Their preferences included improving meaningful consent, extending personal data to online indicators, introducing privacy by design requirements for all products and strict reporting of data breaches.

7.2.1. NGOs at the Commission (GDPR)

Table 7 shows that NGOs performed well at the Commission with each group achieving at least 50% of their preferences indicating that NGOs were more successful at this venue. AN attained the highest score at the Commission, achieving 69% of their preferences (Table 27). As the

Commission initiates the legislative process and drafts the initial proposal, NGOs were satisfied with this initial text. The Commission supported NGO requirements on consent, data minimisation and international data transfer laws. In contrast to business preferences, AN and EDRi secured privacy by design principles in the initial proposal explaining their high score in table 7 (Table 24 & 27). Not all preferences were met at the Commission. AN and EDRi advocated against the main establishment principle, which was ignored by the Commission. It should be noted that this was not a major issue for NGOs, as ANEC and VZBV did not provide an opinion on this issue. ANEC futilely lobbied against the use of certification systems for data processors (Table 25). Overall, the results in table 7 suggest that the Commission favoured many NGO ideologies in shaping this regulation.

7.2.2. NGOs at the Parliament (GDPR)

Table 7 shows that NGOs performed well at the Parliament with AN and EDRi achieving 75% and 63% of preferences respectively. Similarly, to the Commission, AN had its preferences on consent, data minimisation and privacy by design fully met at Parliament (Table 27). An interesting finding shows that when NGOs converged on a preference, they were usually successful as evidenced on their preference for consent and data processing principles. The Parliament used similar language to ANEC advocating principles of fairness, lawfulness and transparency to be incorporated into the legislation (Table 25). The Parliament supported delegating powers to the Commission to ensure compliance and public accountability in reporting data breaches. Table 7 shows that some groups such as VZBV lost out at Parliament as they advocated strict international data transfer laws compared to other groups (Table 27). Overall, the Parliament produced a positive outcome for NGOs.

7.2.3. NGOs at the Council (GDPR)

Table 7 shows that NGOs had a relatively poor outcome at the Council, which affected its outcome in the final regulation. Table 7 shows that the Council was more likely to support business interests compared to NGOs who on average secured just over a third of their preferences at the Council. This had a damaging effect on NGOs with respect to the final regulation with only EDRi and ANEC achieving at least 50% of their preferences. There are several examples which illustrate how Council amendments to the text reduced the success of NGOs. The consumer protection NGOs (VZBV, ANEC) called for a principle of data

minimisation to be included. Whilst the Commission and Parliament supported this, Council removed all text relating to data minimisation principles (Table 25 & 26). The Council did not support ANEC's definition of personal data to specific online identifiers unlike the Commission and Parliament (Table 25). The Council's amendments to the text illustrate a lack of convergence with NGO preferences.

The results in table 7 show that NGOs initially performed well at the Commission and Parliament but lost out in the final regulation due to Council amendments. This could be caused by a lack of lobbying at the Council, or an inability of NGOs to supply necessary resources to gain access to the Council. This case demonstrates how each EU institution can change a policy outcome.

7.3. Business Association preferences in the non-salient case

This section looks at the important preferences of business interests and their success at the three main EU institutions. In general, business associations looked to minimise the adjustment costs they faced in adapting to this regulation. Their preferences included advocating for no regulation, introducing workarounds to existing processes and diluting the severity of the the regulation. Unlike NGOs, the business groups analysed did not converge on all preferences, with many looking for industry specific requirements, especially the telecommunications (GSMA) and banking industry (EBF).

7.3.1. Business associations at the Commission (GDPR)

Table 7 shows a relatively weak performance for business groups relative to NGOs as only AC managed to secure 50% of preferences. The Commission was not responsive to industry-specific requests which explain the low score in table 7 for both EBF and GSMA (Table 30 & 31). Business groups looked for weak regulation on data breach notification requirements and exemptions on user consent which were not realised at the Commission which supported stricter regulation in the initial proposal. Therefore table 7 shows that business interests were initially less satisfied than NGOs.

7.3.2. Business associations at the Parliament (GDPR)

Table 7 shows that most business groups improved their score at the Parliament relative to the Commission, with both DE and AC securing 50% of their preferences. Whilst the Parliament

supported strict regulation on business interests, AC improved its definition of consent at Parliament, seeking exemptions for marketing and scoring purposes (Table 29). It is interesting to note when a business association looked for no regulation, they were relatively unsuccessful. Data breach laws is an interesting example where EBF unsuccessfully lobbied for voluntary reporting of breaches rather than regulation (Table 30). The Parliament was somewhat responsive to creative workarounds suggested by DE (Table 28). Rather than not regulating data breach requirements, DE and AC sought to reduce the notification duties rather than voluntary action which explains their relative higher score at Parliament (table 7).

7.3.3. Business associations at the Council (GDPR)

Table 7 shows business groups had their best outcome at the Council suggesting that it is an important venue for them to lobby. DE and AC performed well here achieving 88% and 69% of preferences respectively (Table 7). The Council supported workarounds advocated by these organisations. Examples include special "work agreements" for processing employee data and the "principle of pseudonymisation" allowing anonymised personal data to be processed freely. The Council used similar wording to AC in their amendment of this principle. (table 29).

7.4. Summary of results for non-salient case (NIS)

Table 8: Results of NIS Directive- Non-salient Directive

Interest Group	Group type	Outcome Commission	Outcome Parliament	Outcome Council	Outcome of Directive
EDRi	NGO	7/16 (44%)	5/16 (31%)	4/16 (25%)	4/16 (25%)
AN	NGO	4/16 (25%)	4/16 (25%)	3/16 (19%)	3/16 (25%)
BoF	NGO	6/16 (38%)	4/16 (25%)	1/16 (6%)	2/16 (13%)
EURid	NGO	8/14 (57%)	4/14 (29%)	5/14 (36%)	5/14 (36%)
AC	BA	8/16 (50%)	11/16 (69%)	9/16 (56%)	11/16 (69%)
EBF	BA	5/16 (31%)	11/16 (69%)	6/16 (38%)	9/16 (56%)
DE	BA	7/16 (44%)	16/16 (100%)	9/16 (69%)	14/16 (88%)
ECA	BA	4/16 (25%)	9/16 (56%)	4/16 (25%)	9/16 (56%)

Own illustration

The NIS directive is relatively short compared to GDPR with 27 articles meaning it was difficult to accommodate preferences made by all groups. This is reflected in table 8 which shows a disparity in preferences attained by NGOs and business interests with the latter achieving a greater outcome in the final directive. In general, business interests out-performed NGOs at the Parliament, Council with a similar result at the Commission (table 8). The following sections will look at the preferences and successes of all interest groups at the three main institutions.

7.5. NGO preference for non-salient case (NIS)

In general, NGOs saw this directive as an opportunity to regulate business and government, improve transparency of online operators, and introduce new accountability measures to include civil society participation and for Europe to become a global leader in designing cyber security policy (Annex III). As the results in table 8 shows, NGOs lost a lot of preferences to private interests. Table 8 shows that while the initial proposal by the Commission slightly favoured NGOs, the final text shifted in favour towards business groups creating a disproportionate win for private interests. The following sections look at this in more detail.

7.5.1. NGOs at the Commission (NIS)

The Commission was the most likely venue for NGOs to have their preferences met. As illustrated in table 8, EDRi and EURid secured 44% and 57% of preferences respectively. EURid achieved a greater outcome at the Commission compared to all other groups. The list of market operators subjected to this directive was the same for both EURid and the Commission (Table 35). NGOs like AN achieved a lower result as they lobbied for all processors of data to be included (Tablet 8 & 33). As table 8 shows no clear pattern with the outcome of the Commission, it suggests that the Commission accommodated both sides.

7.5.2. NGOs at the Parliament (NIS)

Unlike GDPR, the Parliament was less likely to support NGOs with no group achieving one third of their preferences (Table 8). Many NGOs advocated that all processors of personal data and public administration bodies should be under the scope of this directive. The Parliament disagreed, reducing the implication for big-tech companies (Table 32). BoF scored low in table 8, as it lobbied unsuccessfully for public accountability in incident reporting and NGO oversight in managing national cyber security bureaus (Table 34). The Parliament supported the

preferences private interests instead illustrating major disconnect between NGO preferences at the outcome at Parliament.

7.5.3. NGOs at the Council (NIS)

Table 8 illustrates that NGOs had their lowest score at the Council with most groups failing to exceed 25% of their preferences. This can be explained by a clash of interests between NGOs and the Council as NGOs advocated for national government bureaus to be subject to this directive (Table 32). Council ministers did not want their own government to be implicated and amended the text to remove any accountability of public administration (European Council, 2014). NGOs faced difficulties in having their preferences heard at the Council, explaining their low score.

7.6. Business interest preferences for non-salient case (NIS)

Business groups did not want their members to be subjected to this directive as it created adjustment costs for firms. Private interests sought to reduce their duties to EU agencies, introduce clauses to protect their public reputation, and create self-complying mechanisms to reduce the effect of this directive on their processes. Unlike NGOs, business interests did not converge, and were sector-specific which can explain the variation in the results for business groups table 8. Big-tech interests represented by AC and DE performed exceptionally well with the banking (EBF) and telecommunications (GSMA) groups failing to secure sector-specific preferences for its members.

7.6.1. Business interests at the Commission (NIS)

Whilst the Commission had a slight preference towards NGOs, big-tech interests, DE, and AC secured approximately 50% of their preferences at the Commission (Table 8). These groups had achieved their preferences on limited reporting of cyber security breaches integrated into the initial proposal (Table 36 & 38). However, the lack of sector specific clauses in the initial proposal explains why results are lower than at the Parliament (Table 8).

7.6.2. Business interests at the Parliament (NIS)

The outcome at the Parliament shows a clear support of business interests with respect to this directive (Table 8). The Parliament advocated for special treatment of big-tech interests, DE, which resulted in separate articles being created for digital service providers (Table 38). The

Parliament supported adding tools for self-compliance of private firms to the text which was suggested by EBF (Table 37). This explains the figures in table 8 which illustrate a strong performance for EBF and DE at Parliament. DE's high degree of preference attainment in the final directive was heavily aided by its success at Parliament (Table 8).

7.6.3. Business interests at the Council (NIS)

Table 8 shows that certain business groups performed well at the Council. DE and AC performed well here securing 69% and 56% of preferences respectively. However, EBF and ECA were less successful in achieving their desired outcome at the Council. ECA's low score of 25% can be explained by the conflict of interest that occurred between ECA and DE. ECA advocated for incident reporting to focus on products designed digital providers, i.e. DE members, removing accountability from the aviation industry (Table 39). The Council did not support this preference, agreeing with the solution put forward by DE (Table 38).

Table 8 demonstrates a major win for big-tech interests who secured 88% of their preferences, followed by American corporate interests on 69%. It should be noted that several large big-tech firms are members of both DE and AC (Tables 11 & 13). Although it represents U.S. interests in Europe across multiple sectors, AC's preferences were largely in defence of the big-tech industry (Table 36). Similarly, to the GDPR, business interests performed well at later stages in the legislative process as NGOs lost out. Taking EDRi and DE as examples in table 8, where both initially secured 44% at the Commission, EDRi fell to 25% due to legislative amendments and DE improved its result achieving 88% with amendments from the Parliament and Council. The following chapter reflects on these results providing insights on lobbying success.

8. Discussion

This chapter tests the hypotheses formulated in chapter 4 against the results illustrated in chapter 7. Where possible, the data has been presented in graphic format to provide clarity on whether the hypotheses are confirmed or rejected.

8.1 Findings of public salience

Both figure 1 and 2 illustrate preference attainment in percentage format of interest groups at the three main institutions and the final proposal. On the x axis, the first four groups are NGOs and the second four are business associations for both figures.

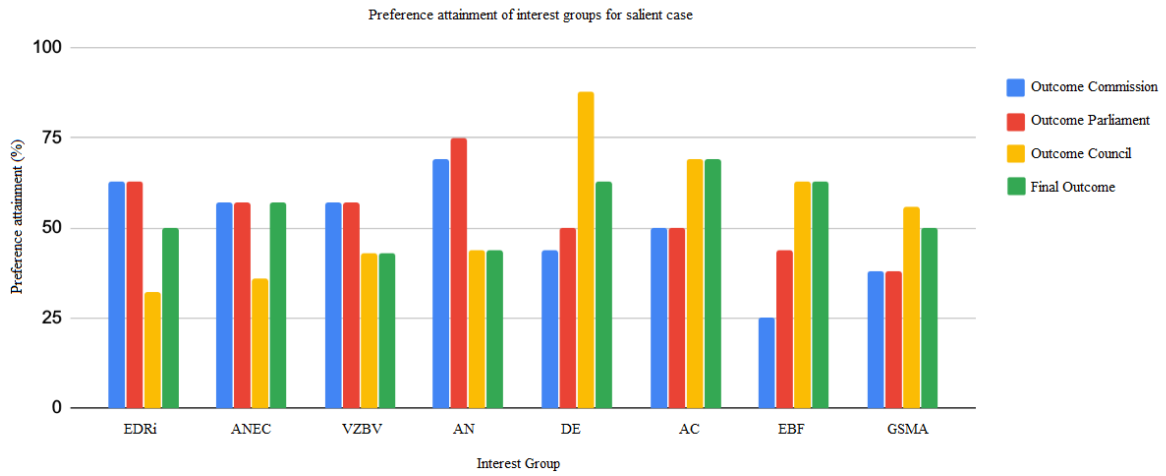

Figure 1: Salient case: Preference attainment for all groups at the three institutions and final directive (GDPR)

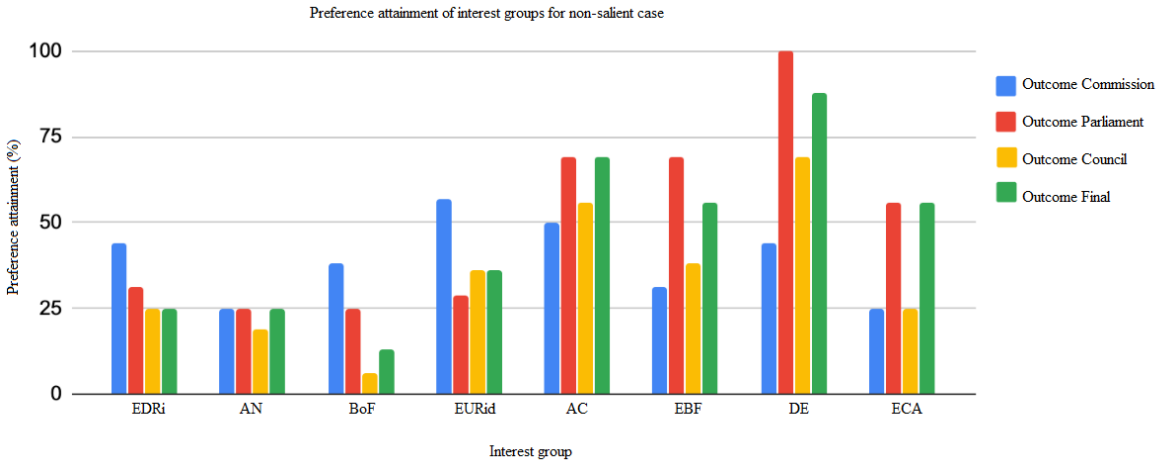

Figure 2: Preference attainment for all groups at the three institutions and final directive (non-salient case NIS)

H1: the more public attention there is on an issue, the less likely an interest group can achieve their desired policy outcome.

Recalling 4.1.1., Mahoney (2007) argues that the public salience of an issue matters when understanding who is influential in the legislative process and who is attaining their preferences.

Mahoney (2007) argues that as public attention increases on an issue, legislators are less likely to listen to one interest group and consider other opinions fearing the threat of public scrutiny for listening to one group only. Therefore, Mahoney (2007) concludes that interest groups are less likely to achieve their desires on salient issues compared to non-salient ones which are not under public scope. While figure 1 shows that NGOs can improve their result under salient conditions, figure 2 shows that business associations can achieve more under non-salient conditions. With respect to digital policy, H1 is rejected as certain groups perform better under salient conditions. The important takeaway is that salience does matter as a pre-condition for interest groups to achieve their desired outcomes with respect to these cases. A logical explanation for this lies in the type of goods groups are seeking. NGOs seek public goods which benefit society compared to business associations which seek benefits for its members (Hix & Hoyland, 2011). When an issue is important to the public, like the GDPR, policymakers are more likely to listen to public interest groups to show solidarity with public interests and support the citizens of Europe. On issues of low salience, they are not under these constraints illustrating a yearning to support private interests. It is important to note that business associations collectively achieved more than NGOs in both proposals. Whilst NGOs improved their score under salient conditions, they did not collectively achieve more than business associations.

8.2. Findings of salience in the parliament

H2: In issues of high salience to the public, the parliament is likely to support public interests to appease their voters.

H2.1: However, in issues of low public salience, the parliament is more likely to satisfy business interests as they are not being scrutinised by the public.

The parliament is directly accountable to the citizens of Europe as it is an elected body. However, Hix and Hoyland (2011) discuss how MEPs seek re-election which results in a varied supporting of interests that are important to its electorate and private business interests as they provide necessary resources for elections. This research examined whether public salience influences the parliament's decision making. Figure 1 indicates that in a climate of high public salience, parliament will support NGOs and figure 2 shows that under conditions of low public salience it supports business interests with respect to these cases. The hypothesis can explain this phenomenon. The NGOs in this research advocate for public goods and the protection of society.

As illustrated through the analysis of the Financial Times, personal data protection was an important issue in European media and therefore important to the general public (Mahoney, 2007). Politicians seeking re-election would be unwise to vote against proposals that aim to protect and support the average voter in favour of interests of large multinationals. This theory does not apply for issues of low public salience like cyber security. Politicians are under less constraint to support public causes favouring profitable organisations that can provide information on voters and finance campaigns (Hix & Hoyland, 2011). The reasoning behind the outcome at the Parliament in both cases can be explained by politicians seeking re-election. Both H2 and H2.1 are accepted in the case of digital policy.

8.3. Findings of interest group type

Table 9 and 10 below illustrate the collective outcome of preferences attained by NGOs and business associations for both directives. For example, in table 9, to calculate the collective success of NGOs in the salient case, the results of the NGOs' success in achieving their preferences in the final proposal are presented in percentage format. The four groups' results are added together to give a collective score for NGOs in the salient case, which is 212. This demonstrates what interest group type is performing better overall rather than individual groups.

Table 8: Lobbying success of the final proposal (Salient case - GDPR)

NGOs	**Preference attained in final proposal (%)**	**Business Associations**	**Preference attained in final proposal (%)**
EDRi	50	DE	63
ANEC	56	AC	68
VZBV	50	EBF	50
AN	56	GSMA	50
Total lobbying success of NGOs	**212**	**Total lobbying success of BA**	**231**

Table 9: Lobbying success of the final proposal (Non-salient case - NIS)

NGOs	Preference attained in final proposal (%)	Business Associations	Preference attained in final proposal (%)
EDRi	33	AC	75
AN	19	EBF	63
BoF	13	DE	88
EURid	36	ECA	56
Total lobbying success of NGOs	**101**	**Total lobbying success of BA**	**282**

H3: Business associations will be more likely to achieve their desired policy outcome compared to NGOs.

H3.1: However, interest groups lobbying for diffuse goods are more likely to be successful in achieving their desired outcome on a highly salient issue compared to those advocating for private interests.

As discussed in chapter 2, Olson's (1965) logic of collective action theory argues that private interests have greater incentive to lobby compared to NGOs due to the potential higher return they can achieve for their members. NGOs lobbying for public interests enjoy a shared societal benefit meaning the goods they receive are non-excludable. This incentivises groups to "free-ride" and not excessively lobby compared to private interest (Olson, 1965). As table 10 and table 11 shows, business associations collectively achieved more of their goals relative to NGOs. For the non-salient case, the disparity between the two types of groups is greater. However, the situation becomes more nuanced through the salient case. Table 10 shows a slight victory for business associations relative to NGOs. As illustrated in 8.1, whilst NGOs perform better under salient conditions, business associations still achieve more of their preferences in both cases. While salience closes the gap between NGOs and business associations, businesses are more

likely to achieve their goals, even under salient conditions. Therefore, hypotheses H3 is confirmed whilst H3.1 is rejected.

8.4. Findings of finance

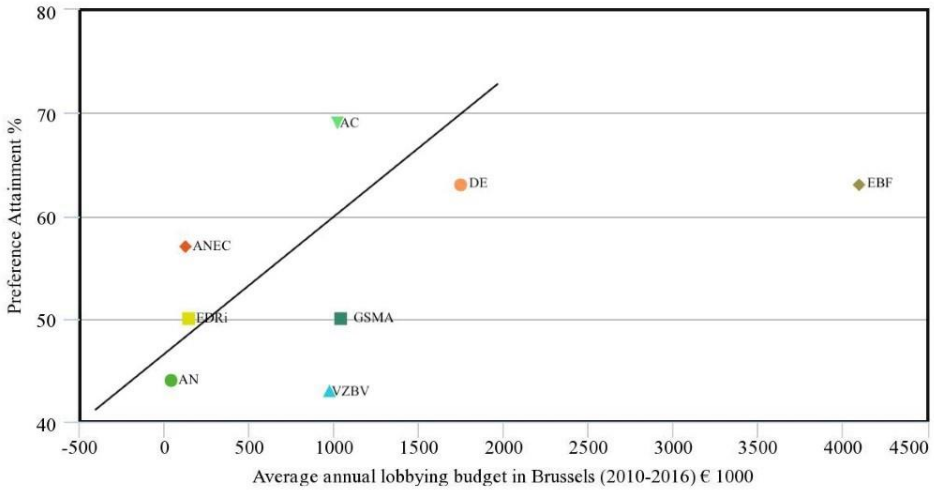

Figure 3: Relationship between annual lobbying spend and preference attainment of interest groups with respect to salient case (GDPR)

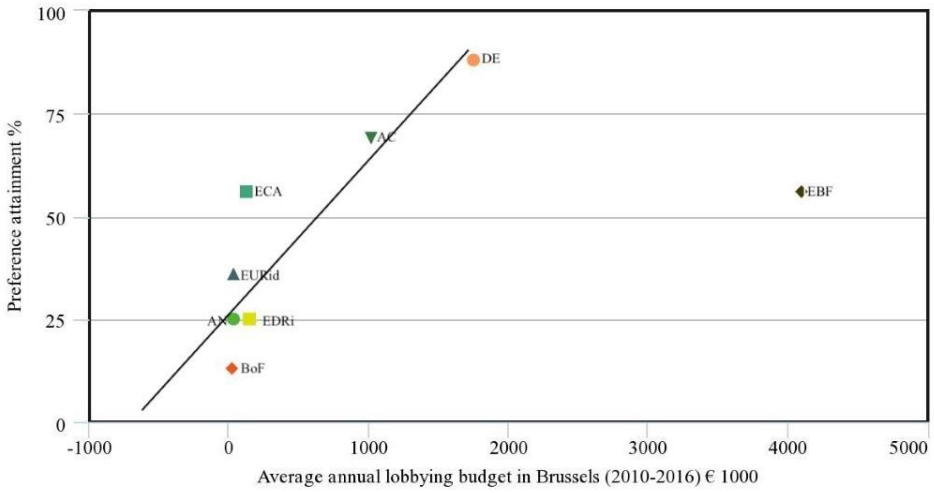

Figure 4: Relationship between annual lobbying spend and preference attainment of interest groups with respect to non-salient case (NIS Directive)

H4: The wealthier organisation will be more influential in obtaining their desired outcome.

Recalling 4.2.22, Eising (2007) argued that organisations with strong financial resources are the most successful in achieving their outcomes. The scatter plots above present the interest groups relative to their annual lobbying spend in Brussels. The black line suggests that as the annual budget of a group increases this should have a positive effect on achieving their preferences. Figures 3 and 4 illustrate interesting findings. Initially, EBF the wealthiest organisation is a clear outlier in both cases. This potentially illustrates that finance has a positive effect until a certain point as EBF did not attain the highest degree of preferences in either case. Atikcan and Chalmers (2019) argue that the financial industry was firmly against the GDPR due high adjustment costs which produced a negative outcome for them. EBF explicitly rejected both proposals which could explain their result. Second, figure 3 illustrates that VZBV achieved the least amount of preferences even though they are the wealthiest NGO. ANEC, a less well-endowed organisation performed the strongest of the NGOs. This suggests that finance is not an important explanatory factor for NGOs achieving their preferences. Third, the linear regression in figure 4 illustrates that most groups sit near the line. This suggests that there is some relation

between financial endowment and preference attainment under non-salient conditions. As illustrated in H2.2, the Parliament is responsive to private, wealthy interests when the public doesn't care about an issue. Applying a similar logic here, it appears that all three institutions favour wealthy interests when public attention is low. This suggests that the EU institutions respond well to money but fear public repercussions. As already stated, the EU must appear democratic and for the people of Europe, not wealthy interests. While these are interesting findings, H4 is rejected as finance does not provide a definitive explanation why some interest groups are performing better than others in both cases. The relationship is stronger under non-salient conditions. This hypothesis could be improved by adjusting it to account for salient conditions.

8.5. Findings of established relationships of interest groups

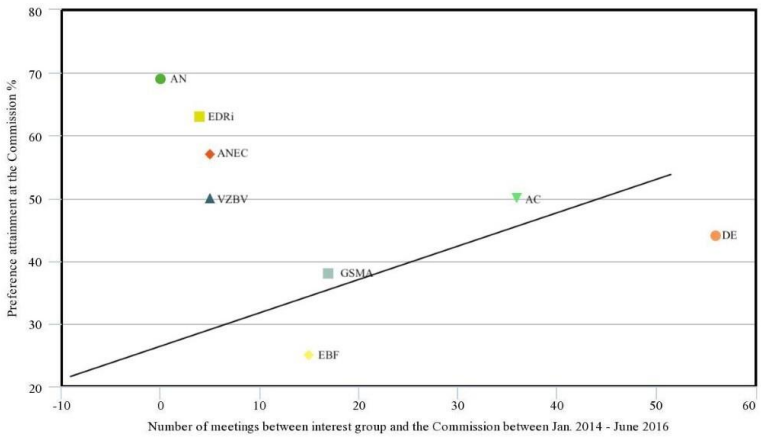

Figure 5: Relationship between meetings at the Commission and preference attainment of interest groups at the Commission with respect to the salient case (GDPR)

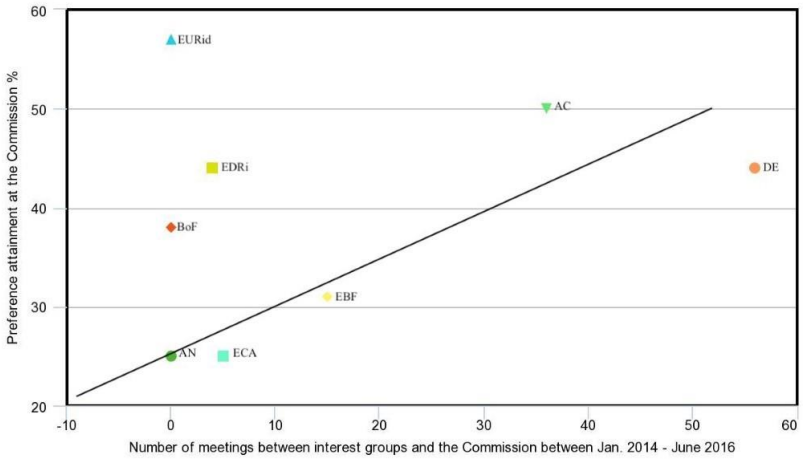

Figure 6: Relationship between meetings at the Commission and preference attainment of interest groups at the Commission with respect to the non-salient case (NIS Directive)

H5: The stronger the relationship is between the lobbyists and institution staff members; the more successful lobby groups will be in achieving their desired outcome.

MyKay (2012) argued that personal connections between lobbyists and governmental administrative staff are important. Interest groups seek to hire former administrative staff due to the access they have to institutions. This research analysed the relationship between official meetings it held at the Commission and the outcome it achieved at that institution. Bunea (2013) argues that measuring preference attainment at the Commission is a good is a solid indicator of the overall process. The results in figure 5 and 6 illustrate that for business associations, preference attainment increases as the group holds more meetings with the Commission. For NGOs, they achieved a high degree of preference attainment without engaging in many formal meetings. There are two potential explanations for this. First, the Commission favours public interest groups with respect to digital policy or second, NGOs are getting access to Commission lawmakers through other platforms such as public consultations and expositions organised by the Commission. The neo-pluralist theory argues that the Commission seeks representation from both private and public interests (Hix & Hoyland, 2011). Therefore, H5 is rejected as preference attainment of an interest group does not increase in line with the number of meetings held at the Commission.

8.6. Findings of Council success

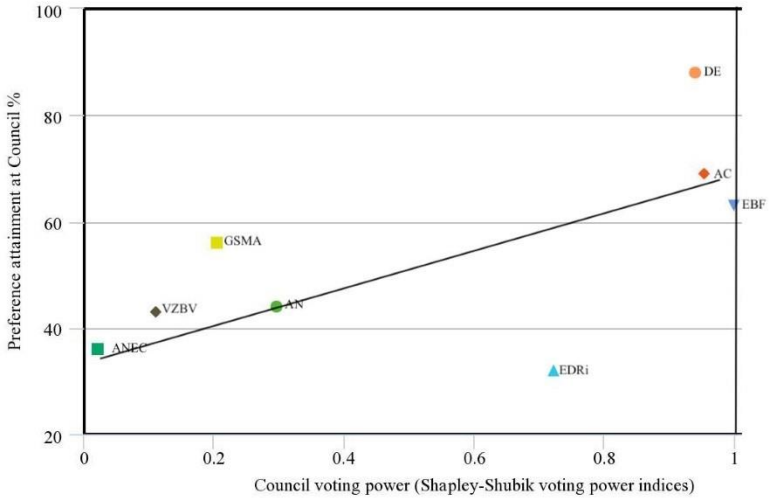

Figure 7: Relationship between voting power at the Council where groups have regional offices and preference attainment of interest groups at the Council with respect to the salient case (GDPR)

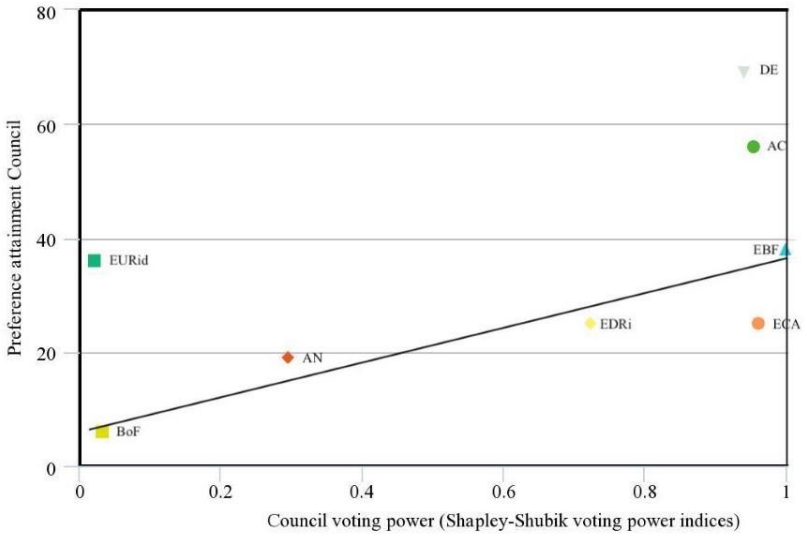

Figure 8: Relationship between voting power at the Council where groups have regional offices and preference attainment of interest groups at the Council with respect to the non-salient case (NIS)

H6: Interest groups with greater lobbying activity in the member state's capitals are more likely to be influential at the Council than interest groups that are Brussels based only.

Derived from Bouwen (2002) and Michowitz (2002), interest groups who successfully lobby national government are likely to have their preferences met at the Council. Groups that have permanent representation in member states were analysed to understand if national presence as a positive effect at the Council. To account for variance of voting power at the Council, the Shapley-Shubik scale taken from Barr and Passarelli (2009) has been used as a measurement.

Looking at figure 7 and 8, it illustrates that business associations have greater national presence across Europe compared to NGOs. This provided a favourable outcome for business associations in the salient case who achieved a high degree of preference attainment at the Council. The Council appears responsive to salience as a pattern emerges along the linear regression line. This is less evident in the non-salient case, illustrated by fig. 8. Whilst a group with large representation across Europe performs well at the Council, salience and interest group type should also be considered to affect a group's outcome at the Council. It would be interesting to measure the outcome of multinational NGOs at the Council to understand if they can achieve a

higher degree of preferences like AC and DE. Therefore, the hypothesis is rejected due to inconclusive data. This research indicates that the Council tends to support American and big-tech interests with respect to digital policy.

8.7. Findings at the Commission

H7: The interest group who can supply the most appropriate policy-relevant information to the Commission is most likely to achieve their desires with the Commission.

From 4.3.2., Michowlitz (2007) illustrates that groups who provide technical information to the EU are likely to be influential. Similarly, Bouwen (2002) states that the Commission seeks policy-relevant expert information to improve the content of their proposals. He demonstrates this by suggesting that financial and banking interest groups can provide the most relevant information on finance-related policy proposals. Applying that logic here, it is assumed that organisations specialising in developing technology and digital infrastructure will be most influential in shaping cyber security and data protection policy. The likely winners should be DE AC and GSMA as their members are the manufacturers and operators of global technological infrastructure which is subject to data protection and cybersecurity concerns (see tables 11, 13 & 15 for relevant members).

As Figure 1 and 2 illustrate, DE, AC and GSMA received their lowest preference at the Commission for both proposals indicating that these groups' potential to supply expert knowledge did not affect the Commission in both cases. This suggests that the Commission is not affected by salience. For both proposals, the Commission was more likely to listen to NGOs over business interests. Recalling Bouwen's (2002) work, it should be noted that the private firms themselves provide the best information to the Commission, rather than the business associations they operate in. As business associations can have many members with conflicting ideas, the policy-relevant information could become diluted. It would be interesting to look at this framework by analysing the preferences of the big-tech firms themselves as they have a strong presence in Europe. An alternative explanation could lie with the neo-pluralist argument illustrating that the Commission listens to both digitally-focused NGOs and business associations to provide expert knowledge. H7 is rejected as a result.

9. Conclusion

This research looked at various factors that are used to explain lobbying success in EU digital policy. Sixteen interest groups were selected and analysed through two legislative proposals, one with high public salience and a second with low salience. A methodology adapted from Mahoney (2007) and Bunea (2013) was used to provide empirical evidence in answering the research question:

To what extent do interest group characteristics, issue-specific characteristics and EU institutional factors explain the influence of interest groups when lobbying on EU digital policy?

This chapter answers the research question, presents the main findings and limitations with conducting this research and gives suggestions for future research. Finally, it suggests how to improve theoretical discussion and interest group lobbying in digital policy and societal implications.

9.1 Main findings and answering the question

The research question looks at finding the variables which explain the success of interest groups in achieving their desired outcomes in formulating EU digital policy. From the literature review, it was deduced that the issue of public salience, specific characteristics of EU institutions and characteristics of the interest groups themselves are important factors to consider in explaining the success of interest groups.

Initially, it was discovered that public salience is an important condition for interest groups to consider when lobbying the Parliament. Under highly salient conditions, NGOs perform better as the Parliament looks to appease voters in matters important to the public. Salience was less important at the Council and even less so at the Commission no clear pattern emerged across the two cases. In general, business associations performed well at the Council and should consider this as a fruitful route to lobby.

Second, interest group type is an important factor to consider in understanding why some interest groups are achieving more than others. This research supports a popular finding in the literature that business interests prevail over public interests in influencing digital policy. Whilst public salience improved an NGO's position, business interests collectively achieved a greater outcome

for their members on both proposals. Financial resources, relationship building, and regional established offices were not found to be strong determinants of lobbying success as groups who did not possess these resources still managed to achieve some of their preferences. However, salience did affect the outcome in some cases illustrating its effect on influence.

It was discovered that interest groups can expect a varied result depending on the institution that they lobby. This research illustrates that interest groups should develop a strategy to lobby as many institutions as possible, throughout the life cycle of the legislative process to improve their outcome. As illustrated with business interests in both processes, they improved their outcome compared to the initial proposal with assistance from the Parliament and Council. As previously mentioned, the Parliament's outcome is affected by public salience. With respect to digital policy, the Commission has a slight preference towards NGOs and the Council has a slight preference towards business associations. This research shows that lobbying happens throughout the legislative process.

Digital policy is quite nuanced compared to other EU policy areas. It is not a winner-takes-all scenario as interest groups can sometimes achieve their desired outcomes without affecting the outcome of a rival group. To summarise an answer to the question, public salience is an important variable to consider, especially with respect to the parliament. For interest-group characteristics, interest groups should consider what type of good they are lobbying for and how this will be received by the Commission and Council. Finance has a positive effect under non-salient conditions. In respect to institutional factors, all three institutions have a role in improving or lowering a group's outcome.

9.2 Limitations

Initially, due to the time-lapse between the legislative process and conducting of this research there was a difficulty in finding data as many documents have been removed or deleted Therefore it was difficult to choose appropriate interest groups that provided preferences. This was especially true in the case of NGOs who provided less written documents than business associations. It was anticipated that interviews would be conducted to improve data results, but no groups were available at the time of writing.

Second, the literature discussion presents other potential variables and measurements that could be used to measure influence. With respect to scope and feasibility of the research, the most appropriate variables derived from theory were chosen. There are other interest group characteristics and alternative indicators that could be used as illustrated in the text. Alternative characteristics include a group's position on the issue and whether they support change or the status quo. With respect to indicators alternative methods to measure relationships such as analysing personal relationships of lobbyists and EU personnel has been discussed in section 5.3.

Third, as illustrated in the literature, measuring lobbying is an estimate as much activity happens behind closed doors. Many meetings, including conciliation committee meetings are not documented. Both cases in this study were subject to these. This is important when considering what impacted the outcome of the proposal and how interest groups might have participated.

Fourth, Dür (2008) reminds the researcher should pay attention to the content of preferences attained. According to Dür (2008) "[i]f a group is successful on 20% of the issues and unsuccessful on 80%, a simple quantitative analysis would suggest that the group has little influence. It may be, however, that the group is successful on all of the issues that are highly salient to it" (p.569). This research should be read with caution as interest groups who achieved low preference scores in this analysis are not necessarily unsuccessful.

Finally, as this was a qualitative case study, the results cannot be generalised to EU policymaking in general. One can expect different results if this framework was applied to monetary or social policy because factors such as expert knowledge, public salience of the issues and the groups participating on lobbying for these issues are different. This means that this research cannot be applied to the general theoretical discussion of EU policymaking. However, it does offer insight into the growing phenomena of EU digital policy and adds to the overall literature on interest group representation at European level.

9.3 Future research

Researchers interested in this field of lobbying should expand the research using a larger number of interest groups and cases. As this research adapted Mahoney's (2007) quantitative method, it can be easily reversed to incorporate a large-N design. It is recommended that a similar research design be conducted using different data sets. As Yin (2009) illustrates, a variety of datasets used

consecutively can improve results. It would be interesting to see the outcome using interviews, surveys, research software and using a new set of interest groups. The scope of the research could be increased to include other types of interest groups; think-tanks, private firms, national agencies etc.

This research illustrates that business interests possess a high degree of authority in obtaining their desires at EU level. This finding could be examined further by adapting this framework to issues of importance to businesses such as monetary policy and regulation affecting the single market.

9.4 Theoretical implications

This research supports the use of research techniques which have been adapted from the literature (Mahoney 2007; Due, 2008; Bunea, 2013). Preference attainment serves as a suitable method to measure preference attainment in a qualitative setting and shedding light on the relationship between several of the independent factors and the dependant factor of interest group success.

Furthermore, this research adds to the academic discourse on interest group representation at EU level. In the case of recent digital policy, Olson's (1965) theory of collection action remains valid; business interests are more likely to achieve their outcomes compared to NGOs representing public interests. This research builds on Mahoney's (2007) work arguing the importance of public salience, especially when measuring influence at the parliament.

This research adds to the discussion of interest group representation at the different institutions (Bouwen, 2002; Michalowitz, 2002; Greenwood 2007). The venue in which an interest group chooses to lobby matters as it is likely to affect its overall outcome. Finally, this research provides interesting discussion on a group's ability to provide expert knowledge to the Commission suggesting a different outcome to that of Bouwen (2002) and Michalowitz (2002).

9.5. Societal implications

There is no doubt that digital infrastructures have caused a revolutionary change in society. The often-tumultuous relationship between technology and politics continues to develop through a balance of regulatory policies supporting transparency and accountability against providing the framework for businesses to protect economic interests. The EU has been cited as a pioneer in

developing suitable policy for the digital age. Society should continue to monitor developments in EU digital policy as this research shows public salience balances influence of business interests with NGOs. This is important for NGOs to remember when lobbying for EU digital policy. Finally regarding EU citizens, European digital policy should be subject to public attention to ensure a fair outcome for European societal interests.

Bibliography

Access Now. (2015). Public Consultation on the contractual public-private partnership on cybersecurity and possible accompanying measures. Retrieved from https://ec.europa.eu/digital-

single-market/en/news/contributions-received-organisations-consultation-contractual-ppp-cybersecurity

Access Now. (2017). Responds to Privacy Shield Review Questionnaire. Retrieved June 09, 2020, from https://www.accessnow.org/cms/assets/uploads/2017/07/AN-PSReviewResponse-1.pdf

Access Now. (2018). Protecting our data and celebrating the GDPR. Retrieved June 09, 2020, from https://www.accessnow.org/protecting-our-data-and-celebrating-the-gdpr/

Access Now. (2018a). Creating a data protection framework: A do's and don'ts guide for lawmakers. Retrieved June 09, 2020, from https://www.accessnow.org/cms/assets/uploads/2019/11/Data-Protection-Guide-for-Lawmakers-Access-Now.pdf

Access Now. (2018b). Data Protection: Why it matters and how to protect it. Retrieved June 09, 2020, from https://www.accessnow.org/cms/assets/uploads/2018/01/Data-Protection-One-pager.pdf

Access Now. (2019). National Digital Identity Programmes: What's Next? Retrieved June 09, 2020, from https://www.accessnow.org/cms/assets/uploads/2019/11/Digital-Identity-Paper-Nov-2019.pdf

AmCham. (2010). AmCham EU response to the Commission consultation on protection of personal data. Retrieved May 2020, from https://web.archive.org/web/20160514080336/http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations/american_chamber_commerce_to_eu_en.pdfhttps://web.archive.org/web/20160514080336/http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations/american_chamber_commerce_to_eu_en.pdf

AmCham. (2013). AmCham EU's position on the Network and Information Security Directive. Retrieved June 09, 2020, from https://www.amchameu.eu/sites/default/files/position_papers/file_20130805_153615_OUa_0.pdf

AmCham. (2014). NIS Directive: Getting the Scope Right. Retrieved June 09, 2020, from http://www.amchameu.eu/sites/default/files/position_papers/file_20141014_172304_UbkqV_0.pdf

AmCham. (2014a). Letter to Minister Pat Rabbitte TD on the NIS Directive. Retrieved June 09, 2020, from https://www.amcham.ie/Amcham/media/SiteMedia/Submissions/NIS-Directive-Submission.pdf?ext=.pdf

ANEC. (2012). ANEC position on the European Commission's proposal for a General Data Protection Regulation (GDPR). Retrieved May 2020, from https://www.anec.eu/images/documents/position-papers/2012/ANEC-ICT-2012-G-059final.pdf

Apollonio, D.E & La Raja, Raymond J. (2004) "Who Gave Soft Money? The Effect of Interest Group Resources on Political Contributions," The Journal of Politics 66, no. 4 (November 2004): 1134-1154.https://doi-org.eur.idm.oclc.org/10.1111/j.0022-3816.2004.00293.x

Aspinwall, M. & Greenwood, J. (1998). Collective Action in the European Union: Interests and the New Politics of Associability, London: Routledge.

Atikcan, E. Ö., & Chalmers, A. W. (2019). Choosing lobbying sides: the General Data Protection Regulation of the European Union. Journal of Public Policy, 39(4), 543–564. Retrieved from https://www.cambridge.org/core/journals/journal-of-public-policy/article/choosing-lobbying-sides-the-general-data-protection-regulation-of-the-european-union/1CD77ACA417E50EC0BA01ADF26E30B0F/core-reader

Barr, Jason & Passarelli, Francesco, 2009. "Who has the power in the EU" Mathematical Social Sciences, Elsevier, vol. 57(3), pages 339-366, May.

Baumgartner, F & Berry, J & Hojnacki, M & Leech, B. (2010). Lobbying and Policy Change: Who Wins, Who Loses, and Why. Bibliovault OAI Repository, the University of Chicago Press. 10.7208/chicago/9780226039466.001.0001.

Bernhagen, P., Dür, A., & Marshall, D. (2014). Measuring Lobbying Success Spatially. Interest Groups & Advocacy, 3(2), 202-218. https://doi.org/10.1057/iga.2014.13

Bernhagen, P., & Mitchell, N. J. (2009). The Determinants of Direct Corporate Lobbying in the European Union. *European Union Politics*, *10*(2), 155–176. doi: 10.1177/1465116509103366

Beyers, J & Kerremans, B. (2007). Critical Resource Dependencies and the Europeanization of Domestic Interest Groups. Journal of European Public Policy. 14. 909-920. 10.1080/13501760701243822.

Beyers, J. Eising R., & Maloney W. (2008) Researching Interest Group Politics in Europe and Elsewhere: Much We Study, Little We Know?, West European Politics, 31:6, 1103-1128, DOI: 10.1080/01402380802370443

Bits of Freedom, (2012). Bits of Freedom's response to Public Consultation on NIS Directive. https://web.archive.org/web/20190623053839/https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=2331

Blatter, J. and Haverland, M. (2012), "Chapter 2 Co-Variational Analysis" in Blatter and (Eds.) Designing Case Studies, Basingstoke: Palgrave MacMillan

Blatter, J. (2014). Chapter 4. Congruence Analysis. In M. Haverland (Ed.), *Designing Case Studies. Explanatory Approaches in Small-N Research* (pp. 144-204). Houndsmills-Basingstoke: Palgrave MacMillan.

Bloomberg. (2016). Tips for U.S. companies in the age of EU GDPR and privacy shield. Retrieved June 09, 2020, from https://www.bna.com/uploadedFiles/BNA_V2/Legal/Pages/Custom_Trials/BLPV/Tips_for_US_Companies_EU_GDPR_Privacy_Shield_final.pdf

Bouwen, P (2002) Corporate lobbying in the European Union: the logic of access, Journal of European Public Policy, 9:3, 365-390, DOI: 10.1080/13501760210138796

Bouwen, P. (2004), Exchanging access goods for access: A comparative study of business lobbying in the European Union institutions. European Journal of Political Research, 43: 337-369. doi:10.1111/j.1475-6765.2004.00157.x

Bunea, A. (2013). Issues, preferences and ties: determinants of interest groups' preference attainment in the EU environmental policy, Journal of European Public Policy, 20:4, 552-570, DOI: 10.1080/13501763.2012.726467

Coen, D. (1997). European Business Lobby. Business Strategy Review, Vol. (8)4: 17-25.

Coen, D. (2007) Empirical and theoretical studies in EU lobbying, Journal of European Public Policy, 14:3, 333-345, DOI: 10.1080/13501760701243731

Cooper, H., & Hirst, N. (2017). Silicon Valley tech lobbyists swarm Brussels. Retrieved June 18, 2020, from https://www.politico.eu/article/silicon-valley-tech-lobbyists-swarm-brussels/

Culpepper, D. (2011) Quiet Politics and Business Power: Corporate Control in Europe and Japan, New York, Cambridge University Press, Cambridge Studies in Comparative Politics.

De Vaus, D. A. (2001). Research Design in Social Research. *Sage*. doi:10.1016/S0020-7489(01)00040-2

DIGITALEUROPE. (2009). Response to European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data. Retrieved June 09, 2020, from https://web.archive.org/web/20160516012752/http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations/digital_europe_en.pdf

DIGITALEUROPE. (2012). Draft DIGITALEUROPE amendments to data protection regulation. Retrieved June 09, 2020, from https://wiki.laquadrature.net/images/c/c4/DIGITALEUROPE_Amendments-to-Data-Protection-Regulation_final.pdf

DIGITALEUROPE (2013) comments on the draft network and information security directive. (2013). Retrieved June 09, 2020, from

https://web.archive.org/web/20190623053839/https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=2331

Dür, A. (2008). Measuring interest group influence in the EU: A note on methodology. European Union Politics, 9(4), 559-576. doi: 10.1177/1465116508095151
Dür, A., & De Bièvre, D. (2007). The question of interest group influence. Journal of Public Policy, 27(1), 1-12. doi: 10.1017/S0143814X07000591

Dur, A., & Mateo, G. (2016). *Insiders versus Outsiders*. London: Oxford University Press.

EDRi (2009). Response to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. Retrieved June 09, 2020, from https://web.archive.org/web/20160517113405/http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations_not_registered/edri_en.pdf

EDRi. (2011). The slide from "regulation" to corporate censorship. Retrieved June 09, 2020, from https://edri.org/wp-content/uploads/2010/01/selfregualation_paper_20110925_web.pdf

EDRi. (2012). ENDitorial: EDRi's initial comments on the Data Protection Regulation. Retrieved June 09, 2020, from https://edri.org/edrigramnumber10-2edri-comments-on-data-retention/

EDRi. (2015). Public consultation on the contractual public-private partnership on cybersecurity and the possible accompanying measures. Retrieved June 09, 2020 https://ec.europa.eu/digital-single-market/en/news/contributions-received-organisations-consultation-contractual-ppp-cybersecurity

Eising, R. (2004). Multi-level Governance and Business Interests in the European Union. Governance, 17(2): 211–246.

Eising, R. (2007) 'Institutional context, organizational resources and strategic choices: Explaining interest group access in the European Union', European Union Politics 8(3), 329-363. doi: 10.1177/1465116507079542

Eising, R, Rasch D & Rozbicka P (2017) National interest organisations in EU policy-making, West European Politics, 40:5, 939-956, DOI: 10.1080/01402382.2017.1320174

EURActiv. (2012) Cybersecurity: Protecting the Digital Economy. Retrieved, 09 June, 2020 https://www.euractiv.com/section/digital/linksdossier/cybersecurity-protecting-the-digital-economy/

EURid. (2012). EURid's response to "Improving Network and Information Security in the EU". Retrieved June 09, 2020, from https://web.archive.org/web/20190623053839/https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=2331

Europa. (2014) L277/11. Official Journal of the European Union. Volume 57. 19 September 2014. Retrieved June 09, 2020, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2014:277:FULL&from=ES

Europa. (2016). Summary report on the public consultation on the contractual PPP on cybersecurity and Staff Working Document. Retrieved June 09, 2020, from https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-contractual-ppp-cybersecurity-and-staff-working-document

European Banking Federation. (2009). EBF response to the Commission's consultation on data protection. Retrieved June 09, 2020, from https://web.archive.org/web/20160517114610/http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations/european_banking_federation_en.pdf

European Banking Federation. (2013). EBF's position on the Commission's proposal for a Directive concerning measures to ensure a high common level of network and information security (NIS) across the European Union. Retrieved June 09, 2020, from https://www.ebf.eu/wp-content/uploads/2017/01/EBF-position-paper-on-the-Commission-proposal-for-a-directive-concerning-NIS-final.pdf

European Banking Federation. (2017). EBF Comments to the working party 29 guidelines on lead supervisory identification one stop shop. Retrieved from https://www.ebf.eu/wp-content/uploads/2017/04/EBF_025583-EBF-comments-WP29-guidelines_Lead-supervisory-identificatio.._.pdf

European Banking Federation. (2018). Article 29 Data Protection Working Party: EBF's comments on guidelines on transparency. Retrieved June 09, 2020, from https://www.ebf.eu/retail-payments/data-protection-art-29-working-party-guidelines-on-transparency-ebf-comments/

European Banking Federation (2018a) Article 29 Data Protection Working Party: EBF's comments on BCRs. Retrieved June 09 2020, from https://www.ebf.eu/retail-payments/data-protection-art-29-working-party-guidelines-on-bcrs-ebf-comments/

European Banking Federation (2019) European Banking Federation. (2019). EBF position on Cyber incident reporting. Retrieved June 09, 2020. https://www.ebf.eu/wp-content/uploads/2019/10/EBF-position-paper-on-cyber-incident-reporting.pdf

European Cockpit Association (2012) Response to Public Consultation on Improving Network and Information Security. Retrieved June 09 2020, from https://web.archive.org/web/20190623053839/https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=2331

European Council (2013). Consolidated Council amendments to the GDPR. Retrieved on 09 June 2020: https://edri.org/files/EP_Council_Comparison.pdf?fbclid=IwAR2zrJa-LH3dGGgpsRzBIxcm8NvexOHhW__Zpn04JHDFX3MDGuYtCDGuI_4

European Council (2014) Council position on NIS Directive presented for interinstitutional dialogue. Retrieved on 09 June 2020: http://data.consilium.europa.eu/doc/document/ST-13848-2014-INIT/en/pdf

European Commission. (2012). Proposal for a Regulation of The European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Retrieved June 14, 2020, from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF

European Commission (2013) Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union Retrieved 09 June 2020 https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

European Commission (2014). Reform of the data protection legal framework. Retrieved 8 May 2014, from http://ec.europa.eu/justice/data-protection/review/index_en.htm

Europa. (2014). Agreement between the European Parliament and the European Commission on the transparency register for organisations and self-employed individuals engaged in EU policy-making and policy implementation. Retrieved June 09, 2020, from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=uriserv:OJ.L_.2014.277.01.0011.01.ENG

Europa. (2020). Transparency and the EU. Retrieved July 10, 2020, from https://ec.europa.eu/transparencyregiser/public/homepage.do

European Parliament, (2013). Draft European Parliament Legislative Resolution for the GDPR. Retrieved on 09 June, 2020: https://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2013-0402&language=EN&fbclid=IwAR0mjrvdJpqw29vunvSnIavKcXna5Q0E-5EGySUoBKzopw2nhbPaFEsXvn0

European Parliament (2014) Draft resolution for High Common Network Information and Security in the EU. https://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0244

European Parliament (2016) Procedure file for GDPR. Retrieved June 09, 2020: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/0011(COD)&l=en

European Parliament (2016a) Procedure file for NIS Directive. Retrieved June 09, 2020: https://oeil.secure.europarl.europa.eu/oeil/popups/printficheevents.pdf?id=618818&lang=en

European Union (2016) General Data Protection Regulation. Retrieved June 09, 2020 https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Union. (2016a). The Directive on security of network and information systems (NIS Directive). Retrieved June 09, 2020, from https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

European Union. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Retrieved June 14, 2020, from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

European Union (2000) The Charter of the Fundamental Rights of the European Union. Retrieved on 09, June 2020: https://www.europarl.europa.eu/charter/pdf/text_en.pdf

European Union, (2014). Official Journal of the European Union. Volume 57. L277/11.

Greenwood, J. (1997). *Representing interests in the European Union*. New York: Basingstoke : Macmillan ; New York : St. Martin's Press.

Greenwood, R., Suddaby, R., & Hinings, C. (2002). Theorizing Change: The Role of Professional Associations in the Transformation of Institutionalized Fields. The Academy of Management Journal, 45(1), 58-80. doi:10.2307/3069285

Greenwood, J. (2007). Interest representation in the European Union. 3rd edition. Basingtoke/Hampshire: Palgrave Macmillan.

GSMA. (2009). GSMA Europe response to the European Commission consultation on the framework for the fundamental right to the protection of personal data. Retrieved June 14, 2020, from https://web.archive.org/web/20160514082405/http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations/gsma_europe_en.pdf

Gschwend, T & Schimmelfennig, F. (2007). Introduction: Designing Research in Political Science — A Dialogue between Theory and Data. Research Design in Political Science, 1-18 Doi: 10.1057/9780230598881_1.

Hix, S. & Hoyland, B. (2011). The political system of the European Union (3rd edition). Palgrave MacMillan.

Hudson, J., Fielding, S. & Ramsay, C.R. (2019). Methodology and reporting characteristics of studies using interrupted time series design in healthcare. *BMC Med Res Methodol* 19, 137. https://doi.org/10.1186/s12874-019-0777-x

Klüver, H. (2011). The contextual nature of lobbying: explaining lobbying success in the European Union. European Union Politics, 12(4): 483–506. doi:10.1177/1465116511413163

Klüver, H. (2013) Lobbying as a collective enterprise: winners and losers of policy formulation in the European Union, Journal of European Public Policy, 20:1, 59-76, DOI: 10.1080/13501763.2012.699661

Levitt, S & Bryceson, S & Mierlo, F. (2017). The EU institutions. DOI:10.1057/978-1-137-55256-3_3.

Locatelli, E. (2017). The role of Internet Wayback Machine in a multi-method research project. *The Role of Internet Wayback Machine in a Multi-method Research Project*. University of London. Retrieved June 14, 2020 https://archivedweb.blogs.sas.ac.uk/files/2017/06/RESAW2017-BruggerLocatelliWeberNanni-Web25.pdf

Lock, A. and Harris, P. (1996) Political Marketing—Vive La Difference. European Journal of Marketing, 30, 28-90. http://dx.doi.org/10.1108/03090569610149764

Lowi, T. (1972). Four Systems of Policy, Politics, and Choice. Public Administration Review, 32(4), 298-310. doi:10.2307/974990

Mahoney, C. (2007). *Lobbying success in the United States and the European Union.* Journal of Public Policy, 27(1), 35-56. doi: 10.1017/S0143814X07000608

Malan, D. (2018, June 21). The law can't keep up with new tech. Here's how to close the gap. Retrieved July 08, 2020, from https://www.weforum.org/agenda/2018/06/law-too-slow-for-new-tech-how-keep-up/

Maloney, W., Jordan, G., & Andrew M. McLaughlin. (1994). *Interest Groups and Public Policy: The Insider/Outsider Model Revisited.* Journal of Public Policy, 14(1), 17-38. Retrieved March 17, 2020, from www.jstor.org/stable/4007561

McKay A, (2012) *Buying Policy? The Effects of Lobbyists' Resources on Their Policy Success.* Political Research Quarterly, Vol. 65, No. 4 (December 2012), pp. 908-923 Sage Publications, Inc. on behalf of the University of Utah. Retrieved June 14, 2020 https://www.jstor.org/stable/41759323

McKinley, M., & Groll, T. (2015). The Relationship Market: How Modern Lobbying Gets Done. *Center for Ethics*. Retrieved June 14, 2020 https://ethics.harvard.edu/blog/relationship-market-how-modern-lobbying-gets-done

Michalowitz, I. (2002). Beyond Corporatism and Pluralism: Towards a New Theoretical Framework, in: Warleigh, A. and Fairbrass, J., (Eds.). Influence and Interests in the European Union: The New Politics of Persuasion and Advocacy. London, Europa Publications: 35-53.

Michalowitz, I. (2007). *What determines influence? Assessing conditions for decision-making influence of interest groups in the EU.* Journal of European Public Policy, 14(1), 132-151. doi: 10.1080/13501760601072719

Mitchell, T. R. (1985). An Evaluation of the Validity of Correlational Research Conducted in Organizations. *The Academy of Management Review, 10*(2), april 1985, 192-205. doi:10.2307/257962

Newman, A. L. (2010). What You Want Depends on What You Know: Firm Preferences in an Information Age. *Comparative Political Studies, 43*(10), 1286-1312. doi:10.1177/0010414010369068

Olson, M. (1965). The logic of collective action: public goods and the theory of groups. Cambridge University, MA: Harvard University Press.

Riege, A. (75). Validity and reliability tests in case study research: A literature review with "hands-on" applications for each research phase. *Qualitative Market Research, 6*(2), 2003rd ser., 86. doi:10.1108/13522750310470055

Schwab, K. (2015, December 12). The Fourth Industrial Revolution What It Means and How to Respond. *Foreign Affairs.* Retrieved June 18, 2020, from https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution

Truman, D. B. (1951). The governmental process. Political Interests and Public Opinion. *New York, Alfred A. Knopf, Inc., 40*(9). doi:https://doi.org/10.1002/ncr.4110400915

Vannoni, M., Dür, A. (2017). Studying Preference Attainment Using Spatial Models. *Eur Polit Sci* 16, 369–382 https://doi-org.eur.idm.oclc.org/10.1057/eps.2016.13

Vidačak, I. (2003). Interest groups and lobbying in the European Union. *Croatian International Relations Review, 9*(33), 177-188. doi:https://hrcak.srce.hr/122723

VZBV. (2009). Answers to the Consultation on the EU General Data Protection Framework. Retrieved on 09 June 2020: https://web.archive.org/web/20160514100543/http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations/vzbv_en.pdf

Wichter, Z. (2018). 2 Days, 10 Hours, 600 Questions: What Happened When Mark Zuckerberg Went to Washington. Retrieved June 18, 2020, from https://www.nytimes.com/2018/04/12/technology/mark-zuckerberg-testimony.html

Woll, C. (2006) Lobbying in the European Union: From Sui Generis to a comparative perspective. Journal of European Public Policy 13 (3): 456–469.

Yin, R. K. (2009). Case study research: Design and methods. Sage Publications.

Appendix I – Information on interest groups

AmCham EU

Founded in 1948, AmCham EU represents American companies who operate in Europe. They focus on trade, investment and competitiveness issues. It represents over 160 countries from a wide range of sectors. It operates regional offices across Europe. Members include Amazon, American Express, Barclays, Cisco, Dell, Facebook, Google, Mastercard, McDonalds, Nike, Salesforce and Coca-Cola illustrating that is represents many big-tech interests as well as other groups

Table 10: : Presentation of variables for AmCham EU

Meetings with Commission (relationship)	36
Lobbying budget	€1,025,000
Type of good sought	Private
Experience (founded)	1948 (AmCham Belgium - later rebranded) http://www.amchameu.eu/about
Transparency register	14/10/2008
Brussels office	Yes
Regional offices (ability to lobby national government)	26 - Austria, Belgium (dedicated office to national government), Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, The Netherlands, Poland, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom. Shapley-Shubik score: 0.954
Expertise (policy relevance)	Yes – Many big-tech companies who are theorised to provide expert knowledge are members of AmCham. However, as it represents other sectors, it is expected that its interests are not as concentrated as other technology business associations.

European Banking Federation

EBF represents the banking sector in Europe representing approximately 3,500 banks. It focuses on issues affecting large and small banks, wholesale, retail, local and international sectors.

Table 11: Presentation of variables for EBF

Meetings with Commission (relationship)	23.8
Lobbying budget	€4,100,000
Type of good sought	Private
Experience (founded)	€4,100,000
Transparency register	19/12/2008
Brussels office	Yes
Regional offices (ability to lobby national government)	Yes – All member states (including the U.K., pre- 2016) Shapley-Shubik score: 1.0
Expertise (policy relevance)	No – for the most part, finance companies do not build bespoke systems opting for systems created by many big-tech companies. This logic is derived from the theoretical framework outlined in Chapter 4

DIGITALEUROPE

DigitalEurope is a business association representing digitally transforming industries in Europe. It aims at growing Europe digitally by attracting and sustaining global technology companies. It represents 35,000 businesses and 73 global corporations. Corporate members include Amazon, Apple, Cisco, Dell, Dropbox, Facebook, Google, Hewlett Packard, Huawei, Mastercard, Microsoft, Oracle, Philips, Samsung, SAP, Sony, Visa, and VMWare. These companies are the creators and operators of some of the global digital infrastructures.

Table 12: Presentation of variables for DigitalEurope

Meetings with Commission (relationship)	9
Lobbying budget	€1,750,000
Type of good sought	Private
Experience (founded)	1999
Transparency register	26/10/2011
Brussels office	Yes
Regional offices (ability to lobby national government)	Yes – All member states (including U.K.) except Bulgaria, Czechia, Latvia and Malta. Shapley-Shubik score: 0.94
Expertise (policy relevance)	Yes – DigitalEurope represents big-tech interests in Europe. Their members are the creators and operators of the digital infrastructure that the EU attempts to regulate

	through EU policy. Technology is their speciality

European Cockpit Association

The ECA represents over 40,000 pilots at EU level. Similarly, to EBF, it represents national associations in Brussels. It focuses on issues of relevance to the aviation industry including cybersecurity, competition, women in aviation and matters pertaining to the European Aviation Safety Agency.

Table 13: Presentation of variables for ECA

Meetings with Commission (relationship)	4.5
Lobbying budget	€124,000
Type of good sought	Private
Experience (founded)	1991
Transparency register	Private
Brussels office	Yes
Regional offices (ability to lobby national government)	Yes – All member states except Poland and Slovakia. Shapley-Shubik score: 0.962
Expertise (policy relevance)	No – specialises in aviation rather than technology in general

GSMA

GSMA is a worldwide organisation representing the interests of 750 mobile operators with 400 additional companies within the eco-system. They lobby on issues such as 5G, internet of things, roaming, security and SIM technology. Their members include Vodafone, Three, Telefonica, T-Mobile and KPN.

Table 14: Presentation of variables for GSMA

Meetings with Commission (relationship)	6.75
Lobbying budget	€1,040,000
Type of good sought	Private
Experience (founded)	1995
Transparency register	Private
Brussels office	Yes
Regional offices (ability to lobby national	Yes – Belgium, Spain, United Kingdom

government)	Shapley-Shubik score: 0.206
Expertise (policy relevance)	Yes – It focuses on technology to telecommunications. Many of its members are key operators and creators of digital platforms. Its expertise is reflected in the policies it focuses on.

NGOs

European Digital Rights Initiative (EDRi)

Table 15: Presentation of variables for EDRi

Meetings with Commission (relationship)	4
Lobbying budget	€150,000
Type of good sought	Public
Experience (founded)	2002
Transparency register	Public
Brussels office	Yes
Regional offices (ability to lobby national government)	Yes – Spain, Ireland, United Kingdom, Sweden, Finland, Denmark, Belgium, Netherlands, Germany, Austria, Italy, Poland, Romania, Bulgaria. Shapley-Shubik score: 0.723
Expertise (policy relevance)	No – whilst they specialise in digital affairs, their expertise is on promoting digital rights rather than specialising in technical knowledge on digital infrastructure itself

Bits of Freedom

Table 16: Presentation of variables for BoF

Meetings with Commission (relationship)	0
Lobbying budget	€24,000
Type of good sought	Public
Experience (founded)	2000
Transparency register	5/7/2012

Brussels office	No
Regional offices (ability to lobby national government)	1 – Netherlands Shapley-Shubik score: 0.033
Expertise (policy relevance)	No – whilst they specialise in digital affairs, their expertise is on promoting digital rights rather than specialising in technical knowledge on digital infrastructure itself

Access Now

Table 17: Presentation of variables for Access Now

Meetings with Commission (relationship)	0
Lobbying budget	€40,400
Type of good sought	Public
Experience (founded)	2009
Transparency register	11/1/2012
Brussels office	Yes
Regional offices (ability to lobby national government)	3 – Belgium, Germany, United Kingdom Shapley-Shubik score: 0.296
Expertise (policy relevance)	No – whilst they specialise in digital affairs, their expertise is on promoting digital rights rather than specialising in technical knowledge on digital infrastructure itself

ANEC

Table 18: Presentation of variables for ANEC

Meetings with Commission (relationship)	5
Lobbying budget	€127,000
Type of good sought	Public
Experience (founded)	1995
Transparency register	30/6/2008
Brussels office	Yes
Regional offices (ability to lobby national government)	No – Brussels based. Shapley-Shubik score: 0.022
Expertise (policy relevance)	No – they specialise in consumer affairs.

Table 19: Presentation of variables for EURid

Meetings with Commission (relationship)	0
Lobbying budget	€40,000
Type of good sought	Public
Experience (founded)	2003
Transparency register	
Brussels office	Yes
Regional offices (ability to lobby national government)	No
Expertise (policy relevance)	No – they specialise in domain registration. They are not the manufacturers of digital infrastructure.

Table 20: Presentation of variables for VZBV

Meetings with Commission (relationship)	5
Lobbying budget	€980,000
Type of good sought	Public
Experience (founded)	2000
Transparency register	
Brussels office	No
Regional offices (ability to lobby national government)	1 – Germany Shapley-Shubik score: 0.111
Expertise (policy relevance)	No – specialises in consumer affairs.

Annex II – Timeline of cases though the legislative process

Table 21: Timeline of main events of GDPR

Date	**Event**
24 October 1995	Directive 95/46/EC of the European Parliament and of the Council
June 2009	DG JUST launches a public consultation on strengthening data protection is launched
25 January 2012	The Commission publishes the legislative proposal for the GDPR. COM(2012)0011
16 February 2012	Civil Liberties, Justice and Home Affairs

	(LIBE) appointed as the responsible committee in the parliament. First reading in the Parliament.
25 October 2012 – 12 February 2016	The GDPR proposal is first debated in the Council (Justice and Home Affairs). (Meeting: 3279) There were 9 Council meetings in total.
12 March 2014	Parliament votes and adopts GDPR, 1st reading
3 September 2014	Interinstitutional negotiations are opened after 1st reading in Parliament
15 June 2015	Council reaches general approach to GDPR. The European Data Protection Board will replace the Article 29 Working Party.
27 July 2015	European Data Protection Supervisor (EPDS) publishes recommendations to EU co-legislators in negotiating the final text of the GDPR in the form of drafting suggestions.
17 December 2015	Approval of text after 1st reading of interinstitutional negotiations
8 April 2016	Council position is published (05419/2016)
14 April 2016	Decision made by Parliament (T8-0125/2016)
27 Apri; 2016	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 is adopted. Repeal of Directive 95/46/EC

Own illustration. Data sourced from EU Parliament Procedure File for GDPR (2016)

Table 22: Timeline of key dates for NIS

Date	**Event**
September 2010	Commission adapts Directive (2013/40/EU) introducing minimal rules on offenses and

	sanctions against attacks on information systems. Commission proposes to strengthen ENISA (526/2013/EU)
July 2012	DG CONNECT launched a public consultation on "Improving NIS in the EU" which would serve in developing the NIS Directive. The Commissioner responsible is Neelie Kroes.
7 February 2013	European Commission published its Cyber Security Strategy which includes a proposed Directive on Network and Information Security 2013/0027 (COD)
20 March 2013	Internal Market and Consumer Protection (IMCO) is appointed as the committee responsible for the NIS Directive. Rapporteur is PPE Andreas Schwab
15 April 2013	The Parliament's first reading of the NIS directive. They approve it for the next stage.
06 June 2013 - 29 February 2016	The NIS Directive is discussed by the Transport, Telecommunications and Energy configuration (Meeting: 3243). There are 4 meetings in total on this directive at the Council.
13 March 2014	Decision by Parliament, 1st reading
6 October 2014	Committee decide to open interinstitutional negotiations after the 1st reading in the parliament
14 January 2016	Approval in committee of the text agreed in at the 2nd reading interinstitutional negotiations
17 May 2016	Council position is published (05581/1/2016)
6 July 2016	Decision by Parliament (T8-0303/2016)
19th July 2016	Publication of the NIS directive in the Official Journal of the EU
November 2018	Deadline for member states to identify businesses operating as essential services

Own illustration. Data sourced from European Parliament Procedure file (2016a)

Annex III – Preferences of interest groups

Table 23: Preferences for EDRi (GDPR)

	Consent	Score
Preference	Defines consent as **"**Consent should always require active behaviour, both in online and offline environments." (EDRi, 2012) Right to withdraw consent (EDRi, 2012)	
Commission	Art. 7 - Controller shall bear the burden of proof for the data subject's consent. Consent of data subject should be given in a written or clear declaration. Right to withdraw consent	2
Parliament	Art. 7 - Consent is a result of choice by the data subject. Suggests that controllers should request frequent re-affirmations of consent. Right to withdraw consent.	2
Council	Art. 7 - The controller should demonstrate that unambiguous consent was given by the data subject. Right to withdraw consent.	2
Final	Art. 6 & 7: consent requires clear affirmative action from the subject. Art. 7(3) - Subject has right to withdraw consent	2
	Rules pertaining to processing of data	
Preference	Stronger principles in ensuring the minimisation of collection and processing of data. Reduce the scope. Data collected should be the absolute minimum needed to fulfil process (EDRi, 2009) Controllers should bear the cost in processing requests from subjects. (EDRi, 2009) Data should be transferred in a format which the subject agrees on especially for former employees	
Commission	Art. 5(1c) - supports data minimisation and scope Art. 12 - Controllers can charge a fee	1
Parliament	Data protection principles should include data minimisation and purpose limitation. (yes) No mention of who should bear the cost in processing such requests. (no).	1
Council	Removes data minimisation from Art 5(1c). No mention of who should bear the cost in processing requests from	0

	data subjects. Member states can impose specific laws for processing employee data in line with human right laws. However, this is not the right of the subject to choose	
Final	Art. 5 1c clarifies data minimisation. Art. 18 states circumstances where data can be deleted Controllers can charge a fee to subjects in requesting data (Art. 15 [3]).	1
	Personal data	
Preference	Increase transparency on how data is collected, where it is stored (EDRi, 2009) Broader definition of "personal data" to include indirect forms of data which could eventually lead to a natural person (EDRi, 2009)	2
Commission	Art. 5 - processed lawfully, fairly and in a transparent manner in relation to the data subject Art. 4 - Personal data definition is vague. It deals with information relating to a subject.	2
Parliament	Art. 5(1a) - personal data needs to be treated lawfully, fairly and transparently. Art. 4(2) - personal data relates to an identified person, directly and indirectly by one or more specific factors.	2
Council	No clear mention on law, fair and transparency in art. 5. Art. 4 - agrees with inclusion from parliament to expand personal data definition to direct and indirect means	1
Final	Art. 5(1)(c) increases transparency Art. 4 defines personal data in direct and indirect forms	2
	Data breaches	
Preference	Remove causes of breach e.g. "breach of security measures" - all breaches should be included Subjects should be informed if their personal data has been compromised. (EDRi, 2012) Create a central public register to report data leakage (EDRi, 2012)	
Commission	Art. 9 - Documents personal data breach as a breach of security. Art. 32 - data breaches need to be communicated to the subject. No public register	1
Parliament	Exemptions are allowed in specific and well-defined public interests (no)	

	Art. 32(1) - includes notifying subjects their rights, privacy or legitimate interests are compromised. (yes) Art. 31(4a) - create a public register for data breaches (yes)	
Council	Art - 31(1) Only breaches which are likely to result in a risk to rights and freedoms of individuals should be reported to the individual (no). Does not support a public register. (no)	0
Final	exemptions to reporting data breaches (art. 34) Art. 34[2] states data breach needs to be informed to subject where their rights are infringed No public register	1
	Main establishment	
Preference	Remove "main establishment" - accountability in all bureaus. Does not support a one representation for multiple undertakings (EDRi, 2011; EDRi 2012)	
Commission	"the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States"	0
Parliament	(13) Supports main establishment, however, provides detailed rules on what constitutes main establishments (no)	0
Council	supports the main establishment principle.	0
Final	(36) lists requirements for the main establishment.	0
	International data transfer	
Preference	Data cannot be requested by companies based in third countries without authorisation from local supervisory authority (EDRI, 2012). Does not support BCRs or safeguards for private companies (EDRi, 2012).	
Commission	Art. 42 - allows for international data transfers through use of BCRs. Stricter Art 45. - no transfers are allowed until the Commission approves that they have adequate levels of protection in accordance with article 41.	1
Parliament	Art. 41 - 42. Delegate specific powers to the Commission to decide if a third country or organisation meets standards. Include a sunset clause where the Commission can revoke allowances. (yes - if the EDRi accepts the Commission as the supervisory authority) Allows for safeguards only where the Commission does not make a decision Art. 43 - supports a regulated, limited scope of BCRs in which the	1

	MS assist in drawing up (no)	
Council	Art. 42 - authorisations are not required from third countries that meet requirements acceptable to the union. Art. 43 - supports the use of BCRs and sets out rules of compliance.	0
Final	Art. 45 permits the use of BCRs, safeguards and certificates by companies which allows for authorisation without further permission from authorities. The Commission has removed its competence to assess third countries and organisations in international cooperation formally in art. 45(2)	0
	Privacy by design	
Preference	Data protection by design to be included. Privacy should be considered at every stage of product development. (EDRi, 2012) Products and services should be certified to meet EU data protection standards (EDRi, 2012) Controllers should use up-to-date technology to empower data subjects access and correction to their data (EDRi, 2009)	
Commission	Art. 23 - Privacy by design is supported. The Commission shall be empowered to adopt delegated acts on this matter. The Commission may lay down technical standards and requirements.	2
Parliament	Art. 23(1) includes "Data protection by design shall have particular regard to the entire lifecycle management of personal data " Art 42(aa) a valid "European Data Protection Seal" for the controller and the recipient in accordance with paragraph 1e of Article 39	2
Council	Art. 23 - removes the obligation of firms to introduce mechanisms on incorporating privacy by design. Rather they need to take measures to ensure compliance. However it is only for areas relating to processing of data and not at every stage of product development. Certification mechanisms are supported in relation to Art. 39.	1
Final	Art. 25 sets out data protection by design. Certification possible under Art. 42. Type of technology used is not specified	1
	Sanctions	
Preference	Civil enforcement should be strengthened (EDRi, 2009) DPAs should be independent from government and agencies. Should be enforced publically. (EDRi, 2009) Range of sanctions available. They should be in line with gross	

	annual turnover of the company. Victims should be compensated when successfully proving a breach of data (EDRi, 2009)	
Commission	Does not strengthen civil participation and enforcement. (no) Art. 77 - right to compensation and liability. Art. 79 - Sanctions are in line with annual turnover. However, it is low between 0.5% and 1% of annual turnover.	1
Parliament	In many instances, the parliament seeks more competences delegated to the Commission (Art. 42, 43 etc). Does not mention civil empowerment. (no) Looks for greater participation of the European Data Protection Board (yes) Art. 79 - higher sanctions in line with GDP of companies. Lists detailed sanctions. (yes) (54) includes Support of compensation of data subject (yes)	1
Council	Does not strengthen civil participation and enforcement. (no) Agrees that sanctions should be in line with gross annual turnover but struggles to find a percentage agreed by the MS. (yes) (118) supports compensation from controller or processor. However, it asks that this be interpreted in the light of the case law of the Court of the EU, reflecting the obligation of the regulation. (yes)	1
Final	Art. 83 - lists range of sanctions Art. 82 - subject can be compensated by controller	1
	Total score Commission	10/16
	Total score Parliament	10/16
	Total score Council	5/16
	Total score final	8/16

Table 24: Preferences for ANEC (GDPR)

	Consent	Score
Preference	Calls for strengthening the requirement of meaningful consent. (ANEC, 2012) Clarify consent of RFID and all IoT systems which are obtained "through signs"	
Commission	Art. 7 – strengthens consent but does not define it with respect to RFID and IoT.	1
Parliament	The parliament expanded on conditions for consent. It must be presented clearly. Supports withdrawal of consent. (yes) No mention of consent through IoT and RFID.	1
Council	Controller should not bear the burden of proof of the data subject's consent but be able to demonstrate that unambiguous consent is	1

	given. (yes) No mention of consent through IoT and RFID.	
Final	Art. 7 states that consent needs to be given by a clear affirmative act, stronger than Directive 95/46/EC Art. 30 states that natural persons can be identified by RFIDs	1
	Rules pertaining to processing of data	
Preference	Seeks transparency processing of data. (ANEC, 2012)	
Commission	Art. 5 – Personal data must be processed in a transparent manner.	2
Parliament	Art. 5 incorporates principle of "transparency" in processing personal data.	2
Council	Art. 5 supports transparent processing of personal data. This was a later addition.	1
Final	Controllers are free to process data once it follows the guidelines of the regulation. There are no standard forms. Art 5 - processing needs to be transparent.	2
	Personal data	
Preference	Personal data needs to be defined in the context of internet of things (IoT) and radio frequency identification (RFID). Add to art. 4.	
Commission	Art. 4 - Specifies online identifier but no mention of RFID ot IoT	1
Parliament	(24) - includes radio RFID and other digital identifiers which can be used to identify a natural person (yes)	2
Council	No mention of RFID or IoT.	0
Final	Art 4. - includes online identifiers. (30) - Online identifiers can include RFIDs.	2
	Data breaches	
Preference	Introduce reporting of personal data breaches, similar to what is in place in electronic communication field (ANEC, 2012)	
Commission	Art. 9 - Documents personal data breach as a breach of security. Art. 32 - data breaches need to be communicated to the subject.	2
Parliament	Art. 31 - supports reporting of data breaches without undue delay.	2
Council	Art. 31 - limited reporting of personal data breaches, where rights are infringed.	1
Final	Personal data breaches need to be reported (33) Art. 33 has a broad scope on broad data breach notification requirements Privacy and electronic communications regulations sit alongside the GDPR.	2
	Main establishment	
Preference	No preference	
Commission		
Parliament		

Council		
Final		
	International data transfer	
Preference	Does not support EU certification schemes in any form as proof of compliance (ANEC, 2012)	
Commission	Art. 42 & 43 - allows for safeguards and BCRs	0
Parliament	Art. 42 & 43 - allows for safeguards and BCRs	0
Council	Art. 42 & 43 - allows for safeguards and BCRs	0
Final	Art 42 - allows for certification as proof of compliance in international data transfer	0
	Privacy by design	
Preference	Include concept of "privacy by design" (ANEC, 2012) Certification of processes needs to be complementary to regulation and not as an alternative	
Commission	Art. 23 – supports privacy by design. Art. 39 - introduces the possibility to establish certification mechanisms. Does not specify it being complementary to duties in accordance with article 23	1
Parliament	Art. 23(1) includes "Data protection by design shall have particular regard to the entire lifecycle management of personal data' Art 42(aa) a valid "European Data Protection Seal" for the controller and the recipient in accordance with paragraph 1e of Article 39 (no)	1
Council	Art. 23 - removes the obligation of firms to introduce mechanisms on incorporating privacy by design. Rather they need to take measures to ensure compliance. However, it is limited to nature, scope, context and purpose of processing data. Certification mechanisms are supported in relation to Art. 39. (yes)	1
Final	Art 25 - includes privacy by design. However, text is altered to refer to practices regarding personal data only. Art 25 - certification is allowed to prove compliance	1
	Sanctions	
Preference	Enforcement mechanisms standardised at EU level. (ANEC, 2012) Provide details on the finances to national authorities should receive so they can carry out enforcement	
Commission	Art. 79 – provides administrative sanctions at EU level. No rules on funding	1
Parliament	Art. 79 - adds a guarantee of harmonisation of sanction within the union No strict rules on funding.	1
Council	Art. 79 - lists detailed sanctions to be standardised at union level. However MS can impose additional sanctions for those not recorded in this regulation. No strict rules on funding.	1

Final	Art 83 - rules on fines No rules on adding additional funding to authorities	1
	Total score Commission	8/14
	Total score Parliament	8/14
	Total score Council	5/14
	Total score final	8/14

Table 25: Preferences for VZBV (GDPR)

	Consent	Score
Preference	Explicit, informed consent needs to be given. No combination of different data sets will be allowed (vzbv, 2009)	
Commission	Art. 7 – Commission prefers wording of explicit consent. Burden lies with the controller to show that the subject agreed to consent.	2
Parliament	Art. 7(2) Includes wording that consent needs to be presented clearly. Any cases which are partly violated are considered void.	2
Council	Art. 7(2) consent needs to be clearly distinguishable from other matters.	2
Final	Art. 7(2) - consent is presented in a clear manner which is distinguishable from other matters.	2
	Rules pertaining to processing of data	
Preference	Supports data minimisation. Only data which is agreed by the customer can be processed. Asks for clarification on cloud technology being used to store data.	
Commission	Art. 5 – supports the data minimisation principle. No mention of cloud technology.	1
Parliament	Art. 5 - supports purpose limitation, data minimisation, accuracy for direct and indirect data processing. (yes) Art. 5 - Data needs to be processed in a way in which the subject can exercise their rights. (yes) No inclusion of cloud technology use (no)	1
Council	Art. 5 - removes data minimisation in prcoessing. (no) There was a debate among many council members whether there should be provisions made with respect to cloud computing. However, they were never included (EDRi, 2014) (no)	0
Final	Art 6(a) - subject must give consent for data to be processed. Art 5 - processing needs to be transparent. Cloud computing was not specifically mentioned.	1
	Personal data	
Preference	Personal data can be used to score potential customers. This should not be allowed. Customers should be able to remove or replace their data in this	

	respect.	
Commission	Art. 5(e) - allowances made for storing personal data for scoring purposes. Art. 5 – supports principle of erasure.	1
Parliament	Does not make allowances for scoring of data. (yes) Art. 5(d) - data must be accurate, can be removed where necessary. (yes)	2
Council	Art. 5(e) Data can be kept and used for statistical purposes Art. 5(d) data can be erased or rectified without delay.	1
Final	No provisions made for scoring. Art. 5(d) - data must be accurate, up to date, and rectified and erased where desired by the subject	1
	Data breaches	
Preference	Personal data breaches need to be reported. They are currently seen as a minor offence; this needs to be challenged and increased. VZBV call for the highest form of sanction in this regard.	
Commission	Art. 32 - data breaches need to be communicated to the subject. The Commission enforces sanctions for failure to complete duties.	2
Parliament	Art. 31 - supports reporting of data breaches without undue delay. Art. 79 - The Parliament is strict on sanctions for infringement of breaches.	2
Council	Art. 31 - limited reporting of personal data breaches, where rights are infringed. Art. 79 - breaches are sanctioned but considers previous offences and nature of breaches.	1
Final	Personal data breaches need to be reported (33) Art. 31 has a broad scope on broad data breach notification requirements Lower level fines are applied for infringements of Art. 33 & 34.	1
	Main establishment	
Preference	No preference	
Commission		
Parliament		
Council		
Final		
	International data transfer	
Preference	Does not support safe harbour frameworks. When it comes to infringements, consumers are unable to improve their rights.	
Commission	Art. 42 & 43 - allows for safeguards and BCRs These are regarded as safe harbour frameworks.	0
Parliament	Art. 42 & 43 - allows for safeguards and BCRs. These are regarded as safe harbour frameworks.	0
Council	Art. 42 & 43 - allows for safeguards and BCRs.	0

	These are regarded as safe harbour frameworks.	
Final	Art 42 - allows for certification as proof of compliance in international data transfer	0
	Privacy by design	
Preference	Supports the idea of being "technology neutral". It is unrealistic otherwise and will hamper innovation.	
Commission	Art. 23 – supports privacy by design. Delegates future powers to the Commission to enact future rules.	0
Parliament	Art. 23(1) includes "Data protection by design shall have particular regard to the entire lifecycle management of personal data' Art 42(aa) a valid "European Data Protection Seal" for the controller and the recipient in accordance with paragraph 1e of Article 39 (no)	1
Council	Art. 23 - removes the obligation of firms to introduce mechanisms on incorporating privacy by design. Rather they need to take measures to ensure compliance. However, it is limited to nature, scope, context and purpose of processing data. Certification mechanisms are supported in relation to Art. 39. (yes)	1
Final	Art 25 - includes privacy by design. However, text is altered to refer to practices regarding personal data only. Art 25 - certification is allowed to prove compliance	0
	Sanctions	
Preference	Clear sanctions available. Equip data protection authorities with the manpower and resources they need (vzbv, 2009)	
Commission	Art. 79 – sanctions laid out clearly. No strict rules on funding.	1
Parliament	Art. 79 - Sanctions available. No strict rules on funding.	1
Council	Art. 79 - Sanctions available. No strict rules on funding.	1
Final	Art 83 - rules on fines No rules on adding additional funding to authorities	1
	Total score Commission	7/14
	Total score Parliament	8/14
	Total score Council	6/14
	Total score final	6/14

Table 26: for Access Now (GDPR)

	Consent	Score
Preference	Explicit, informed consent accompanied with the purpose for which the data will be used. There are no exceptions to this. (Access Now, 2018) Right to withdraw consent.	

Commission	Art. 6 – data subject gives consent for processing of personal data for one or more specific purposes	2
Parliament	Art. 7(2) Includes wording that consent needs to be presented clearly. Any cases which are partly violated are considered void. Art. 5(1b) Supports purpose limitation of collecting consented data Art. 7(3) - supports the right to withdraw consent.	2
Council	Art. 7(2) consent needs to be clearly distinguishable from other matters. Art. 5(1b) supports purpose limitation, except for statistical, scientific or historical purposes. Art. 7(3) - supports the right to withdraw consent.	1
Final	Art. 7(1): request for consent needs to be clear and informative. Art. 7(3) - Subject has right to withdraw consent	2
	Rules pertaining to processing of data	
Preference	Data processing should process necessary data to complete tasks. No other data should be used. (Access Now, 2019) Users have the right to access, rectify and erase their data (Access Now, 2019)	
Commission	Art. 5 - supports data minimiastion Art. 5(e) - supports erasure of data	2
Parliament	Art. 5 - supports purpose limitation, data minimisation, accuracy for direct and indirect data processing. Art. 5 - Data accuracy calls for the right of erasure and rectification.	2
Council	Art. 5 - removes data minimisation in prcoessing. (no) Art. 5 - Users have the right to erase data (yes)	1
Final	Art. 5 1c clarifies data minimisation. Art. 5d states circumstances where data can be deleted	2
	Personal data	
Preference	The regulation should provide greater control for the user over their personal data in private, professional, or public life (Access Now, 2018) Government should not be shielded from personal data requirements (Access Now, 2018b)	
Commission	Art. 5 – lays down the rights of the data subject including better control of data through several principles. Art. 84 – supports obligations of secrecy	1
Parliament	Art. 5 provides greater control through the principles laid out (yes) Art. 84 - Supports obligations of secrecy.	1
Council	Art. 5 provides better control except data minimisation (no) Art. 84 - Supports obligations of secrecy.	1

Final	Art. 5 sets out principles relating to the processing of personal data in all respects of the subject. No special provisions for government. Art. 89 & 90 - There are safeguards in place. Obligations of secrecy is left as a competence to the MS. However ethical obligations are outlined.	1
	Data breaches	
Preference	Measures to address, remedy and notify users on data breaches need to take place. (Access Now, 2019) All breaches should be reported to users. (Access Now, 2019)	
Commission	Art. 32 - data breaches need to be communicated to the subject.	2
Parliament	Art. 31 - supports reporting of data breaches without undue delay.	1
Council	Art. 31 - limited reporting of personal data breaches, where rights are infringed	2
Final	Art. 34[2] states data breach needs to be informed to subject Art. 31(1) allows organisations to assess whether breaches risk the rights and freedoms of natural persons and whether they should be notified or not.	1
	Main establishment	
Preference	Avoid the main establishment principle to remove forum shopping by firms seeking favourable conditions in certain MS. This will damage consistency. (Access Now, 2018a)	
Commission	(27) - supports the main establishment principle.	0
Parliament	(13) Supports the main establishment, however, provides detailed rules on what it characterises as a main establishment to reduce venue shopping. This was the issue at Access Now was trying to fix.	1
Council	(27) supports the main establishment principle. Provides vague cases where the main establishment can be established for a group of undertakings	0
Final	(36) lists requirements for the main establishment. Access Now notes that this practice puts the onus on a few data protection authorities e.g. Irish DPC to uphold the principles of GDPR rather than cooperation at EU level (Access Now, 2019)	0
	International data transfer	
Preference	Does not support any privacy shield agreements or special arrangements between data transfer between the EU and US (Access Now, 2017)	
Commission	Art. 42 & 43 - allows for safeguards and BCRs Art. 40 & 41 - Does not allow for special agreements. Commission approval needed. The Commission can delegate future powers to itself to monitor the relationship with third	1

	countries	
Parliament	Art. 42 & 43 - allows for safeguards and BCRs. These are regarded as safe harbour frameworks, especially in the case of the EU - U.S. relationship.	0
Council	Art. 42 & 43 - allows for safeguards and BCRs. These are regarded as safe harbour frameworks. These are regarded as safe harbour frameworks, especially in the case of the EU - U.S. relationship.	0
Final	Art. 45 permits the use of BCRs, safeguards and certificates by companies which allows for authorisation without permission from authorities. This allowed for the EU-US Privacy Shield (Access Now, 2017)	0
	Privacy by design	
Preference	Supports the principle of "privacy by design" (Access Now 2018a; Access Now 2019). Privacy procedures need to be incorporated from early stages of design. Should be applicable to IT systems, business practices and physical design	
Commission	Art. 23 – supports privacy by design and should be incorporated from inception of produce design	2
Parliament	Art. 23(1) includes "Data protection by design shall have particular regard to the entire lifecycle management of personal data' Art. 23(1a) - Supports data privacy by design is required for all future public tenders. This means it needs to be applied to all utilities.	2
Council	Art. 23 - supports privacy by design. It removes the obligation of firms to introduce mechanisms on incorporating privacy by design. Rather they need to take measures to ensure compliance. However it is limited to nature, scope, context and purpose of processing data.	1
Final	Art. 25 sets out data protection by design. Certification of existing practices and technology is possible under Art. 42. Type of technology used is not specified	1
	Sanctions	
Preference	Data protection authorities must not hesitate in enforcing GDPR through investigations and adequate fines. MS (Denmark and Estonia) should update laws to allow for monetary fines easily (Access Now, 2019)	
Commission	Art. 67 - European Data Protection Board should be set up to monitor compliance through reports	1

	No provisions made for court laws to be changed.	
Parliament	Art. 67 - European Data Protection Board should be set up to monitor compliance through reports No provisions for Denmark and Estonia case - not deemed as a conflicting issue	1
Council	Art. 67 - European Data Protection Board should be set up to monitor compliance through reports No provisions for Denmark and Estonia case - not deemed as a conflicting issue	1
Final	Art. 83 - lists a range of sanctions including fines. Denmark and Estonia system requires court assistance (Access Now, 2019)	1
	Total score Commission	11/16
	Total score Parliament	12/16
	Total score Council	7/16
	Total score final	7/16

Table 27: Preferences for DIGITALEUROPE (GDPR)

	Consent	Score
Preference	Definition should replace consent is "explicitly" given with "unambiguously" (DE, 2012) Seeks exemptions to consent in relation to employees in a particular firm (DE, 2012)	
Commission	Consent requires explicit action. Art. 7(4) - consent does not provide a legal basis for processing where an imbalance exists between data subject and controller. This was seen in relation to employees and employers Art. 82 - allows member states to create their own laws on processing on employment context. This is not an EU competence.	0
Parliament	25) - uses consent should be given"explicitly" in their definition. (124) Parliament allows for processing of employee data under agreement between the employee and management. (yes)	2
Council	(25) - Council replaces "explicitly" with "unambiguously" in the text (yes) (124) National law or collective agreement, including "works agreements" may provide for specific rules on processing of employees' personal data doe employment context	2
Final	Art. 4(11) - changed accordingly (155) "works agreements" can be created which specifies grounds to process employee data, on the consent of the employee	2
	Rules pertaining to processing of data	

Preference	Suggests the appointment of Data Processing Officers to ensure systems work accordingly with data processing principles. (DE, 2009) Firms are free to hire DPOs without constraint. Companies with DPOs should be exempt from registrations and notifications with DPAs (DE, 2009) Recommends voluntary certification systems to promote accountability (DE, 2009)	
Commission	Art. 35 - Supports the role of data protection officer for multinationals. Art. 37 - Commission is given powers further criteria, certs, tasks, and roles. for DPOs.	1
Parliament	(75a) - allows for data protection officers but sets our specific qualifications they must have (no) (77) - allows for a "European Data Protection Seal" as legal certainty for controllers. (yes)	1
Council	(60c) - guidance for implementing appropriate measures can be found through a firm's data protection officer. Does not specify rules about qualification standards for DPOs. (60c) - guidelines to ensure correct data processing can include approved certifications by the EU.	2
Final	Art. 37 - sets out rules on DPOs for multinationals and other firms Art 42 - BCR rules can be used as demonstrating compliance	2
	Personal data	
Preference	Remove online identifiers and location data in definition of personal data (DE, 2012)	
Commission	Recital 24 states that location data may not constitute personal data.	2
Parliament	Art. 4(2) - definition includes location data but not online identifier.	1
Council	Art. 4(2) - definition includes online identifier but not location data.	1
Final	Art 4(1) - contains terms	0
	Data breaches	
Preference	Delete reporting timeframe of 24 hours. Incorporate "without undue delay" in notifying processors of data (DE, 2012) Data breaches are reported only when remedies are found as not to disrupt the organisation (DE, 2012) Removal of any power the Commission has to specify future criteria for data breaches (DE, 2012)	
Commission	Art. 31 - breaches must be reported within 24 hours. Art. 31(4) - Commission has the power to specify future criteria.	0
Parliament	(67) - breaches should be notified without undue delay, which is	1

	presumed to be not later than 72 hours (yes) Art. 34(4) - Delegates powers to the European Data Protection Board	
Council	(67) - amends 24 hours with 72 hours. (68a) - personal data breaches do not need to be reported to the subject if the controller has implemented the appropriate technological protection measures. Art. 34(8) - deletes delegated acts to the Commission for future proposals (yes)	2
Final	Art. 33 - timeframe of 24 hours is replaced with 72 hours. Art. 33(2) - without undue delay incorporated in notification Art. 33(5) - enacting further powers to the Commission is deleted.	1
	Main establishment	
Preference	Define main establishment with respect to processor and controller (DE, 2012) A group of undertakings can nominate one main establishment (DE, 2012)	
Commission	Art. 4 - sets out competence for the main establishment with respect to processor and controller. Art. 51 - the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States	2
Parliament	Art. 4 - Defines main establishment however it does not differentiate between controller and processor (no) Allows for main establishment and details wide criteria for firms to meet in nominating their main establishment. (yes)	1
Council	Art. 4 - defines the main establishment with respect to the processor and the controller. (yes) Allows for nuance when nominating the main establishment with respect to processors and controllers (yes)	2
Final	Art 4(16) - defines main establishment with respect to both terms (36) - one main establishment for a group unless processing purposes are different. DE had issue with this comment	1
	International data transfer	
Preference	Safeguards should be implemented to allow companies to process data on a worldwide basis. (DE, 2009) Promotes the use of binding corporate rules (BCRs) as a certification system to promote accountability. (DE, 2009)	
Commission	Art. 42 & 43 - allows for safeguards and BCRs.	1

	Art. 45 - Transfers outside the scope of the regulation need to be approved by the Commission	
Parliament	Art. 42 & 43 - allows for safeguards and BCRs. Art. 45 - Transfers outside the scope of the regulation need to be approved by the Commission	1
Council	Art. 42 & 43 - allows for safeguards and BCRs.	2
Final	Art. 42 - allows for certification seal for companies to process data. Art. 47 - sets out provisions for BCRs	2
	Privacy by design	
Preference	Keep the status quo. Technology neutral. Directive should not discriminate against a type of technology. (DE, 2009)	
Commission	Art. 23 - Privacy by design is supported. The Commission shall be empowered to adopt delegated acts on this matter. The Commission may lay down technical standards and requirements.	0
Parliament	Art. 23(1) includes "Data protection by design shall have particular regard to the entire lifecycle management of personal data" Art. 23(1a) - Supports data privacy by design is required for all future public tenders. This means it needs to be applied to all utilities.	0
Council	Art. 23 - supports privacy by design. It removes the obligation of firms to introduce mechanisms on incorporating privacy by design. Rather they need to take measures to ensure compliance. However it is limited to nature, scope, context and purpose of processing data.	1
Final	Art 25 - includes privacy by design. However, text is altered to refer to practices regarding personal data only. Certification procedures are possible under art. 42	1
	Sanctions	
Preference	Harmonised across the EU. Sanctions should be harm-based focusing on the fundamental rights of EU citizens (DE, 2009) Recommends setting up a dispute resolution body using commercial and not-for-profit entities. (DE, 2009) Should not include high fines of 4% of revenue. (Bloomberg, 2016)	
Commission	Art. 79 - sanctions are harmonised at EU level. Art. 38 - dispute resolution procedures are a competence of the Commission and national authorities. Business associations can	1

	issue an opinion. (no) Calls for fines of annual turnover of 1%.	
Parliament	Art. 79 - sanctions are harmonised at EU level.(yes) Art. 38 - Dispute resolution procedures shall be conducted by the Commission, MS and authorities (no) Calls for fines of 5% of annual turnover.	1
Council	Art. 79 - sanctions are harmonised at EU level. However MS can impose additional sanctions for those not recorded in this regulation. Art. 38(1a) - Dispute resolution procedures can be drawn up by associations representing categories of controllers and processors.	2
Final	Art 83 - rules on sanctions are laid out clearly. However 4% fines are included as a maximum point. Art. 40(k) - associations representing controllers and processors may set up out-of-court proceedings and resolution procedures resolving disputes between subjects and controllers.	1
	Total score Commission	7/16
	Total score Parliament	8/16
	Total score Council	7/16
	Total score final	10/16

Table 28: Preferences for AmCham (GDPR)

	Consent	Score
Preference	Define consent at European level, especially in the case of the employee. (AmCham, 2010) Consent provides legal grounds to process data in some circumstances e.g. marketing (neither yes or no) Technical solutions can be used to document unambiguous consent	
Commission	Consent of employee laws are left to member states. Does not state marketing as a legitimate interest. Subject's have the right to object to marketing. Technical solutions can be used to document consent.	1
Parliament	Defines consent. (25) Technical solutions can indicate clear affirmative consent (yes) Consent is always required. The mere use of a service does not constitute consent (no)	1
Council	Defines consent. (25) Technical solutions can indicate consent. (yes)	1

	(39) The processing of personal data for marketing purposes can be regarded as a legitimate interest (yes)	
Final	Art 4(11) - harmonises definition of consent at EU level. Art 7 - consent only to process data for that particular contract. Not a legal basis to legitimise future processing without unambiguous consent. However, (47) states that the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest. The subject can cancel this at any time they wish. (32) - Technical solutions are used to document unambiguous consent	1
	Rules pertaining to processing of data	
Preference	Supports the appointment of DPOs to simplify the role for controllers. DPOs can represent multiple member states. DPOs act as substitutes to notification duties. Improve definition of "controllers" and "processors" and harmonisation across member states (AmCham, 2010) Art. 28 - includes an article clarifying the role and obligations of the controller and processor. This was a new addition from 95/46/EC.	
Commission	Art. 35 - Supports the role of data protection officer for multinationals Art. 37 - Commission is given powers further criteria, certs, tasks, and roles. for DPOs. DPOs do not substitute organisations from notification duties on breaches. Art. 35 - A DPO can represent a group of undertakings.	1
Parliament	Recital 75a allows for data protection officers but sets our specific qualifications they must have. This takes away the freedom of private firms. (no) DPOs do not substitute organisations from notification duties on breaches. Art. 35(2) - A group of undertakings may appoint a main responsible DPO, provided that they are easily accessible from each establishment.	1
Council	Article 36 introduces the position and role of DPOs with respect to controllers and processors. Article 37 - the Council removed most text about the tasks of the	1

	DPOs. This is left to the employer. DPOs do not substitute organisations from notification duties on breaches. Art. 35(2) a group of undertakings may appoint one DPO.	
Final	DPOs are permitted for multinationals. Art. 37 - A single DPO can represent multiple undertakings DPOs do not substitute organisations from notification duties on breaches.	1
	Personal data	
Preference	The processor should have access to the link which connects a data source to the natural person to be constituted as personal data. Allow for provisions where data can be processed where there is no clear link between data and natural person, although it could be found in future. (AmCham, 2010)	
Commission	No provision made for pseudonymisation.	0
Parliament	Art. 33 - The Parliament added a safeguard of pseudonymisation to impact assessment forms for data breaches only.	2
Council	France added the obligation of pseudonymisation. The council added a definition into Art. 4 and it to Rectial 23, art. 5, 6, 14, 20, 23, 30, 38 demonstrating a strong support	0
Final	Art. 4(5) - introduces the concept of pseudonymisation. Several provisions are listed to allow companies to process this data	2
	Data breaches	
Preference	Reporting incidents should take a harms-based approach in line with human rights. (AmCham, 2010) (Art. 33 - not harms based) (art. 34 - harms based)	
Commission	Art. 31 - all incidents on personal data breaches must be reported	1
Parliament	Art. 31 - supports reporting of all data breaches without undue delay.	0
Council	Art. 31 - limited reporting of personal data breaches, where rights are infringed.	2
Final	Art. 33 - personal data breaches must be notified to the DPA within 72 hours. Art. 34(1) - breaches need to be reported to the subject when the breach risks their rights	1
	Main establishment	
Preference	Specification of companies with multiple bureaus. Harmonised approach in establishing what constitutes main	

	establishment (AmCham, 2010)	
Commission	Art. 4 - supports the main establishment.	2
Parliament	Art. 4 - supports the main establishment principle. Applies detailed criteria harmonising the rules at EU level. Includes specification for multiple bureaus i.e. multiple undertakings.	2
Council	Art. 4 - supports the main establishment principle and harmonised approach at EU level.	2
Final	Art. 4 - Defines main establishments as regard to controllers and processors with establishments in more than one member state and provides special rules for them.	2
	International data transfer	
Preference	"White list" of third countries. White list should include The United States. Use of certification such as BCRs to demonstrate compliance (AmCham, 2010)	
Commission	Art. 42 & 43 - allows for transfer through safeguards and BCRs Special arrangements can be made for third countries. Transfer of data outside the scope of this directive requires further Commission approval (Chapter V)	2
Parliament	Text added to Recital 80 indicating the Commission can make allowances to specific third countries and revoke them. Art. 42 & 43 - allows for safeguards and BCRs.	2
Council	Art. 42 & 43 - allows for safeguards and BCRs. Text added to recital 81 which allows for sector specific rules in a third country.	2
Final	The Commission can decide that certain third countries hold adequate levels of protection and will not require authorization (Art. 45) Art. 45(7) - allows for sector specific rules which are outlined in the Official Journal of the European Union. Art.42 & 47 - Certification methods to demonstrate compliance including BCRs	2
	Privacy by design	
Preference	Retain the status quo of technology neutrality from 95/46/EC Protection of data should be technologically neutral Flexible approach for future innovations (AmCham, 2010)	
Commission	Supports privacy by design. Art. 23 - Privacy by design is supported. The Commission shall be empowered to adopt delegated acts on this matter.	0

	The Commission may lay down technical standards and requirements.	
Parliament	Supports privacy by design. Art. 23 - It affects the entire life cycle of data processing for a firm. However recital 66 argues that regulation should be technological neutral and support innovation. Solutions are required to have a European Data Seal of Protection.	1
Council	Supports privacy by design. Recital 66 - Council removes working on technological neutrality.	0
Final	Art 25 - includes privacy by design. However, text is altered to refer to practices regarding personal data only. Certification is possible under art. 42.	1
	Sanctions	
Preference	Common approach to sanctions across MS. Revenues obtained by sanctions should be returned to those affected. Should not benefit the government. (AmCham, 2010)	
Commission	Art. 79 - Common approach to sanctions across MS. Recipients of GDPR fines vary. However the state can benefit monetarily	1
Parliament	Art. 79 - Supports regulated sanctions across the union. Recital 54 & 83 - subjects have the right to claim compensation. Recipients of GDPR fines vary. However the state can benefit monetarily	1
Council	Art. 79 - Supports regulated sanctions although member states can impose further sanctions if not available in this text. Recipients of GDPR fines vary. However the state can benefit monetarily.	1
Final	Art 83 - rules on sanctions are laid out clearly. The UK promises to use fines obtained to fund healthcare (ITGovernance, 2018). Art. 82 sets down right to compensation and liability for those who have their rights infringed.	1
	Total score Commission	8/16
	Total score Parliament	8/16
	Total score Council	11/16
	Total score final	11/16

Table 29: Preferences for EBF (GDPR)

	Consent	Score

Preference	Seeks exemptions requirements for consent. This includes intra-group transfer, legitimate marketing, access to additional employees in specific cases. (EBF, 2009) Intra-group transfer is allowed once the data subject cannot be identified.	
Commission	Art. 82 - Consent of employee laws are left to member states. Does not state marketing as a legitimate interest. Subjects have the right to object to marketing	0
Parliament	(39b) - exemptions are made for direct marketing Parliament did not make provisions for group of undertakings (no)	1
Council	(39) - exemptions made for direct marketing. Council agreed that employee and client data in a group of undertakings can be considered under the "legitimate interest" of the controller.	2
Final	Art. 7 - Consent must be clearly given for every action. (47) The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest. (48) - employee personal data can constitute a legitimate interest. This includes intra-group transfers. Art. 5 - Consent cannot be rolled in with other contractual terms. Art. 11 - where the controller no longer needs to identify the data subject in processing data, they can process data without obligation of this regulation.	2
	Rules pertaining to processing of data	
Preference	Data protection laws should be clarified at EU level. However they do not support the strict rules attributed to this regulation. EBF does not believe that the EU needs regulation on data processing. (EBF, 2009) National data authorities should provide written legal guidelines (EBF, 2009) Compliance of firms should be done through self-regulation and non-binding guidelines supplied by EU	
Commission	Supports regulation. Art. 46 - Member states will work with European Data protection board Art. 66 - The Board will issue guidelines. No support for self-regulation.	1
Parliament	Supports regulation. In most cases, the Parliament entrusts the European Data Protection Board with the task of issuing guidelines. (art. 8, 9, 30, 31, 44, 66, 67)	1

	No support for self-regulation	
Council	Supports regulation. The Council tasks the European Data Protection Board to write guidelines (rec. 60, 96, art. 66, 67) No support for self-regulation	1
Final	Regulation harmonises data protection laws across the EU. Member states must transpose it directly into law. Whilst BCRs (Art. 47) and certifications (Art. 42) Firms are legally bound to follow the guidelines	1
	Personal data	
Preference	Data protection laws should be clarified at EU level. Asks for clarification on personal data protection obligations under anti-money laundering framework (EBF, 2009)	
Commission	No provisions made for anti-money laundering.	0
Parliament	The Parliament includes derogations in recital 87 for financial supervisory authorities to prevent money laundering	2
Council	The Council adds text to Recital 16 which restricts obligations on personal data with respect to an anti-money laundering framework.	2
Final	(19) allows member states scope to introduce specific measures in relation to anti-money laundering. However, this is not precise, and interpretation is allowed by MS	1
	Data breaches	
Preference	Non-binding tools and self-regulation (EBF, 2009) The difference between significant and non-significant data breaches need to be identified and remedied accordingly. (EBF, 2017) Data breaches should be reported once the controller is confident a breach has occurred (EBF, 2017) Breaches should not be notified until the cause of breach has been established. (EBF, 2017)	
Commission	Does not support self-regulation. Art. 31 - all breches need to be reported within 24 hours.	0
Parliament	Does not support self-regulation. Art. 31 - supports reporting of all data breaches without undue delay. Does not differentiate between significant and non-significant from a notification and remedy purpose. According to article 31, breaches must be reported within 72 hours.	0

Council	Does not support self-regulation. Art. 31 - limited reporting of personal data breaches, where rights are infringed. Differentiates between types of breaches. According to article 31, breaches must be reported within 72 hours.	1
Final	Art. 34 - Breaches which impose a risk to the rights and freedoms of individuals need to be reported. Art 33 - Data breaches are reported once the DPO can confirm a breach has occurred.	1
	Main establishment	
Preference	Recommends a main establishment approach. All interaction between the firm and DPA should be through that main establishment. (EBF, 2017)	
Commission	Art. 51 - the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States	2
Parliament	Art. 54a - includes an amendment supporting the lead authority clause where a firm can nominate one DPA for all interactions. However the European data protection board has authority to reject a firm's nomination of their preferred authority (no)	1
Council	Art. 51a(1) - includes a clause on the lead authority. This illustrates that all interaction between firms and DPA is through the main establishment bureau, regardless of where the cases are in the union (yes)	2
Final	Art. 56 - the lead authority rule discusses the relationship between the main establishment and the lead supervisory authority.	2
	International data transfer	
Preference	Provide a clear legal framework on processing data from third member states (EBF, 2009) Introduce BCRs to demonstrate compliance (EBF, 2018) Should not apply to data subject to internal decision making between EU and third country units of the same firm (EBF, 2018a)	
Commission	Art. 42 & 43 - allows for safeguards and BCRs. Art. 45 - Intra-group transfers outside the scope of the BCR require approval from the Commission depending on the country it is going to.	1
Parliament	Text added to Recital 80 indicating the Commission can make allowances to specific third countries and revoke them. Art. 42 & 43 - allows for safeguards and BCRs.	1

	Art. 45 - Intra-group transfers outside the scope of the BCR require approval from the Commission depending on the country it is going to.	
Council	Art. 42 & 43 - allows for safeguards and BCRs. Text added to recital 81 which allows for sector specific rules in a third country. BCR rules allow for intra-group transfer.	2
Final	Art. 45 provides a framework. Art. 47 allows for BCRs Art. 45 provides stricter guidelines on intra-data transfer	2
	Privacy by design	
Preference	Keep the status quo - no introduction of privacy by design. Technology neutral and future proof as circumstances change (EBF, 2018)	
Commission	Supports privacy by design. Art. 23 - Privacy by design is supported. The Commission shall be empowered to adopt delegated acts on this matter. The Commission may lay down technical standards and requirements.	0
Parliament	Supports privacy by design principle. Art. 23 - It affects the entire life cycle of data processing for a firm. Solutions are required to have a European Data Seal of Protection. Recital 66 - Parliament supports technological neutrality.	1
Council	Supports privacy by design. Recital 66 - Council removes technological neutrality.	0
Final	Art. 25 - introduces privacy by design. (15) - protection of natural persons should be technologically neutral and should not depend on the techniques used	1
	Sanctions	
Preference	Non-binding regulation	
Commission	Supports sanctions under regulation	0
Parliament	Supports sanctions under regulation	0
Council	Supports sanctions under regulation	0
Final	Sanctions for non-compliance	0
	Total score Commission	4/16
	Total score Parliament	7/16
	Total score Council	10/16
	Total score final	10/16

Table 30: Preferences for GSMA (GDPR)

	Consent	Score
Preference	Consent is only required when the processor needs to identify the subject. Data needed for statistical analysis should not require consent. (GSMA, 2009)	
Commission	Art. 10 - controller is not obliged to acquire additional information in order to identify the data subject. There are many exceptions to this. Art. 83 - processing for statistical analysis requires consent from the subject.	0
Parliament	Parliament adopted recital 88 which states that data which is processed for statistical purposes is exempt from the regulation. Parliament agrees in article 4 that a subject can be identified indirectly, requiring consent.	1
Council	Council added text to recital 23 arguing that the regulation does not include information for statistical and research purposes. Council agrees in article 4 that subjects can be identified indirectly, and consent might be required.	1
Final	Art. 4(1) - A subject can be identified indirectly. Consent might be required in other cases. Not clear. Art. 9(j) - processing for statistical purposes is possible once the rights of the data subject are protected. However, it is circumstantial and will require consent in cases.	1
	Rules pertaining to processing of data	
Preference	Transparent data processing. Obligations should apply to responsible parties that process data of mobile users, irrespective of a business' infrastructure and services. This is to reduce the onus of mobile carriers for services that use their platform (GSMA, 2009)	
Commission	Art. 26 & 27 sets out rules for processing under the authority of the controller and processor.	2
Parliament	Art. 26 - parliament added text indicating that the processor and controller are free to determine respective roles. They allow for instances where the determining party under the scope of the regulation can change.	2
Council	The Council re-wrote article 26 to illustrate contractual clauses between controllers and processors. Whilst a contract is possible, it must be done so in writing.	2

Final	Art. 28 - includes an article clarifying the role and obligations of the controller and processor. This was a new addition from 95/46/EC.	2
	Personal data	
Preference	Personal data should not refer to location data, anonymous web profile, IP address.	
Commission	Recital 24 states that location data is not considered personal data where they do not identify an individual. Data subject can be identified by location data according to art. 4.	1
Parliament	Parliament added online identifiers as personal data to Art. 4.	0
Council	Recital 24 states that location data is not considered personal data where they do not identify an individual. However under Art. 4, location data is personal data.	1
Final	Art. 4(1) - personal data includes information relating to online identifiers etc.	0
	Data breaches	
Preference	Private firms should be accountable to their customers and notify them of issues. This could be mentioned in their privacy statements. No regulation needed here. Firms are accountable already. Argues against formal notification procedures to users. (GSMA, 2009)	
Commission	The Commission supports regulation for data breach notification requirements.	0
Parliament	The Parliament supports regulation for data breach notification requirements.	0
Council	The Council supports regulation for data breach notification requirements.	0
Final	Art. 33 - personal data breaches must be notified to the DPA within 72 hours. Art. 34(1) - breaches need to be reported to the subject when the breach risks their rights	0
	Main establishment	
Preference	Supports methods in reducing bureaucracy of multinationals and their reporting duties to multiple DPAs. (GSMA, 2009)	
Commission	Art. 4 - defines the main establishment. Art. 51 - the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all	2

	Member States	
Parliament	Supports principles of main establishment and lead authorities to reduce administration for firms with multiple bureaus (art. 4 & 54)	2
Council	Supports a clause on the lead authority. This illustrates that all interaction between firms and DPA is through the main establishment bureau, regardless of where the case is located in the union (Art. 51a(1)) - (yes)	2
Final	Art. 4 - Defines main establishments as regard to controllers and processors with establishments in more than one member state and provides special rules for them.	2
	International data transfer	
Preference	Allow firms to assess their own risk and come up with their own technological solutions to assess the risks of individuals. (GSMA, 2009) Supports the use of BCRs to ensure data is transferred globally safely.	
Commission	Art. 42 & 43 - supports safeguards and BCRs. Art. 45 - anything outside of the scope of this regulation is subject to the Commission's approval. The Commission increases the role for the European Data Protection Board in coming up with solutions.	1
Parliament	Art. 42 - Safeguards are allowed but everything requires the European Data Protection Seal which could omit certain technological solutions Supports the use of BCRs	1
Council	Art. 42 - Supports safeguards. Lists rules but no data protection seal is required. Supports the use of BCRs	2
Final	Art. 36 - impact assessments to be conducted with the assistance of the DPO of that firm. Art.42 & 47 - Certification methods to demonstrate compliance including BCRs	2
	Privacy by design	
Preference	Legislation should be flexible to allow for technological and business realities. Does not support Privacy by design. Should not stifle innovation. (GSMA, 2009)	
Commission	Art. 23 - Supports privacy by design. The Commission can lay down future requirements for companies to follow.	0
Parliament	Art. 23 - Parliament includes "Data protection by design shall have particular regard to the entire lifecycle management of personal data from collection to processing to deletion, systematically	0

	focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data." Does not add certifications to prove compliance and supports future delegated acts to the Commission.	
Council	Art. 23 - Council mentions the processes of data processing only, collecting data and anonymity. Supports a limited privacy by design. Supports certification mechanisms and removes removes future delegated tasks of the Commission	1
Final	Art 25 - includes privacy by design. However, text is altered to refer to practices regarding personal data only.	1
	Sanctions	
Preference	Self-regulatory codes and mechanisms. Keep the status quo of art 17 & 27 of Directive 95/46/EC (GSMA, 2009)	
Commission	Supports regulatory sanctions	0
Parliament	Supports regulatory sanctions	0
Council	Supports regulatory sanctions	0
Final	Art 83 - rules on sanctions are laid out clearly.	0
	Total score Commission	6/16
	Total score Parliament	6/16
	Total score Council	9/16
	Total score final	8/16

Table 31: Preferences for EDRi (NIS Directive)

	Scope	Score
Preference	EDRi mentions private and public sectors. Large firms due to their scale. SMEs due to their vulnerabilities. Specific interest should be paid to government databases, due to the amount of personal data they contain. (EDRi, 2015) However, EDRi does stress the importance of including large firms such as SDPs and cloud technology. (EDRi, 2015)	
Commission	Art. 6 - includes public administration Chapter IV - Security of NIS of Public Administration and Market Operators. Certain SMEs are included in the explanatory memorandum of this directive proposal.	2
Parliament	Recital 4a calls to omit public administration. SMEs are also omitted.	0

Council	Council agrees that a greater number of entities concerned with NIS should be included. However for the purposes of harmonisation, they include a minimum list. Council removes public administration from scope.	0
Final	Annex II & III has a limited scope. Public administrations and SMEs are omitted. Annex III - DSPs are included	1
	Member state cyber security bureaus	
Preference	Does not support the establishment of a single CIRT. No single entity should manage cybersecurity. It needs to be delegated amongst multiple agencies in member states. Many states, e.g. Germany already does this. Centralising this process would be unconstitutional. Should be a collaborative and transparent process between all stakeholders and civil society organisations. (EDRi, 2015)	
Commission	Art. 7 - Allows for one CSIRT in every member state. No inclusion of civilian authorities.	0
Parliament	Art. 7 - supports CERTs. Allows for multiple CERTs but all under the same mandate. Art. 6 - supports the inclusion of one or more civilian national competent authorities on the security of NIS.	2
Council	Art. 7 - Supports CSIRTs. Agrees with EDRi that multiple entities within the state can manage the process and should not be left to one state. Does not support civilian inclusion.	1
Final	Does not support the establishment of a single CSIRT. No single entity should manage cybersecurity. It needs to be delegated amongst multiple agencies in member states. Many states, e.g. Germany already does this. Centralising this process would be unconstitutional. Should be a collaborative and transparent process between all stakeholders and civil society organisations. (EDRi, 2015)	1
	Type of incidents to be reported	
Preference	Incidents should be reported to protect the user. Incentives should be introduced to encourage companies to be more transparent and report more incidents. (EDRi, 2015)	
Commission	Art. 14(2) - incidents which have a significant impact on the security of the core services provided by the operator must be reported.	0
Parliament	Recital 8 - reporting of ***"incident having a significant impact"***	0

	means an incident affecting the security and continuity of an information network or system that leads to the major disruption of vital economic or societal functions Art. 14a - refers to core services of the provider. Does not increase the scope of incident reporting. Incidents are reported to the authorities.	
Council	Art. 14(1) & (1a) - incidents related to continuity of essential services need to be reported. Replaces core services with essential. Art. 3a- "essential services" means economic and societal services essential for the functioning of the internal market.	0
Final	No incentives have been introduced through this directive. Incident reporting relates to essential services of operators and not how users consume the service	0
	Accountability of operators of essential services	
Preference	The priority needs to be letting the end user know. This process needs to be transparent and public (EDRi, 2015)	
Commission	Art. 14 - The competent authority can require the OES to inform the public if it believes the incident is of public interest. However the onus is on the authorities to decide on how to act.	1
Parliament	Art. 14 (4) - the public may need to be notified in some circumstances. This is a very limited scope. However the authorities will protect the name of the market operator concerned.	0
Council	Art. 14 - The competent authority can require OES to publish incidents relating to specific individuals.	1
Final	Incidents are reported to CSIRTs. Government can ask providers of essential services to provide additional information if required. Art 14(6) - CSIRTs can notify the public if it is deemed absolutely necessary. However there is no obligation to do so.	0
	Direction of cybersecurity	
Preference	Should be stricter than current worldwide rules on NIS, hardware, applications security (EDRi, 2015)	
Commission	Art. 16 - The Commission will draw up a set of standards relevant to NIS.	2
Parliament	Art. 16 - "***without prescribing the use of any particular technology,*** shall encourage the use of ***European or international interoperable*** standards."	0
Council	Art. 16 - encourages internationally accepted standards without prejudice to technological neutrality.	0
Final	Art. 19(1) - promotes internationally accepted standards in promoting NIS.	0

	No incentives for companies exist in the legislation	
	Penalties	
Preference	EDRi have consistently fought for removal of self-regulation of firms. They advocate for MS to have a wide range of sanctions available to ensure firms comply (EDRi, 2011)	
Commission	Art. 17 - member states can lay down their own sanctions and must report them to the Commission once they have been agreed on	2
Parliament	Parliament supports penalties as demonstrated in article 17. However they will only apply where the OES has truly failed. If they follow steps to rectify the situation, they will not be fined.	1
Council	Art. 17 - agrees that member states can lay down their own rules.	2
Final	Art. 21 - MS shall apply penalties on infringements. They shall be effective, proportionate and dissuasive.	2
	Actions to be taken by operators	
Preference	Incorporate safeguards into products and processes (EDRi, 2015) Should ensure consumer trust. Companies should be incentivised to promote transparency (EDRi, 2015)	
Commission	Recital 25 - products do not have to be designed, developed or manufactured in a particular manner. Does not provide incentives.	0
Parliament	Art. 16 - Parliament includes Member States***, "without prescribing the use of any particular technology,*** shall encourage the use of ***European or international interoperable*** standards and/or specifications relevant to networks and information security" Does encourage transparency in recital 14, and in art. 3 calls for voluntary publishing of cybersecurity incidents to the public in certain sectors	1
Council	Art. 16 - supports technological neutrality. Does not provide incentives.	0
Final	(51) - technology products do not need to be designed, developed or manufactured in a particular manner. No such incentives exist in this legislation	0
	Risk assessment	
Preference	Disapproves of self-regulation of corporations and advocates for a civil society approach in assessing risk (EDRi, 2011; EDRi, 2015)	
Commission	Does not support a civilian national authority to monitor the situation	0

Parliament	(22) - Supports a close cooperation and trust between OES and authorities. It is a collaborative effort. Supports a civilian national authority being established.	1
Council	Art. 1 - The Council supports notification procedures by OES. Cooperation groups are issued with yearly reports on incidents to monitor the situation. Does not support a civilian national authority to monitor the situation	0
Final	(44) - Risk assessment is conducted by the OES. Art. 7 - MS will define objectives for OES to follow. Civil groups are not mentioned in drafting these.	0
	Total score Commission	7/16
	Total score Parliament	5/16
	Total score Council	4/16
	Total score final	4/16

Table 32: Preferences for Access Now (NIS Directive)

	Scope	Score
Preference	All sectors that contain personal data should be included. Specific focus on government databases. (Access Now, 2015)	
Commission	Chapter IV - Security of NIS of Public Administration and Market Operators. Certain SMEs are included in the explanatory memorandum of this directive proposal. Not directed at sectors that contain personal data.	1
Parliament	Recital 4a calls to exclude public administration. Limited scope in Annex II & III.	0
Council	Does not include public authorities in Annex II.	0
Final	Limited scope mentioned in Annex II & III	0
	Member state cyber security bureaus	
Preference	Decrease powers of intelligence and security agencies. It is undemocratic and contradicts human rights freedoms (Access Now, 2015)	
Commission	Art. 7 - establishes a CSIRT in every member state.	0
Parliament	Art. 7 - supports CERTs. Allows for multiple CERTs but all under the same mandate. Art. 6 - supports one or more civilian national competent authorities	1

Council	Art. 7 - supports CSIRTs and does not support civilian intervention in competent authorities.	0
Final	Chapter II establishes a network of CSIRTs in all member states and increases the power of authorities.	0
	Type of incidents to be reported	
Preference	All incidents affecting the end user which is in line with their right to privacy. (Access Now, 2015)	
Commission	Art. 14(2) - incidents which have a significant impact on the security of the core services provided by the operator must be reported.	0
Parliament	Recital 8 outlines the types of incidents that need to be reported. - reporting of "***"incident having a significant impact" means an incident affecting the security and continuity of an information network or system that leads to the major disruption of vital economic or societal functions"*** Art. 14a - refers to core services of the provider. Does not increase the scope of incident reporting. Incidents are reported to the authorities.	0
Council	Art. 14(1) & (1a) - incidents related to continuity of essential services need to be reported. Replaces core services with essential. Art. 3a- "essential services" means economic and societal services essential for the functioning of the internal market.	0
Final	Art 14(3) - only incidents that have significant impact on the continuity of essential services they provide need to be reported	0
	Accountability of operators of essential services	
Preference	Data breaches should be made known to end users and not the government. Government is not accountable to end users. (Access Now, 2015)	
Commission	Art. 14 - The competent authority can require the OES to inform the public if it believes the incident is of public interest. However the onus is on the authorities to decide on how to act.	1
Parliament	Art. 14 (4) - the public may need to be notified in some circumstances. However the authorities will protect the name of the market operator concerned. While the Parliament agrees that the public may need to be informed, the priority has to be protecting the reputation of the firm.	0
Council	Art. 14 - The competent authority can require OES to publish incidents relating to specific individuals.	1

Final	Art. 14 - incident notifications need to be reported to the competent authority or the CSIRT. The government has the onus to notify the public if it will rectify the situation. Personal data breaches follow the rules of the GDPR but are not explicitly mentioned	0
	Direction of cybersecurity	
Preference	cybersecurity policy should take guidance from privacy frameworks, including the International Principles on the Application of Human Rights to Communications Surveillance EU should take the leadership on this, as was the case with GDPR. The NIS directive should also take a user-centric focus like the GDPR (Access Now, 2015)	
Commission	Art. 16 - The Commission will draw up a set of standards relevant to NIS. The Commission agrees that the EU should take leadership in this. However it says it will write guidelines in line with best NIS standards and specifications. There is no mention of human rights in this section.	1
Parliament	Art. 16 - "***without prescribing the use of any particular technology,*** shall encourage the use of ***European or international interoperable*** standards." (31) The Parliament adds that anything with respect to data protection must be in accordance with data protection law. Agrees with the inclusion of the Charter of Fundamental Rights of the EU but not Principles on the Application of Human Rights to Communications Surveillance.	1
Council	Art. 16 - encourages internationally accepted standards without prejudice to technological neutrality.	0
Final	(75) - the directive respects the rights and principles of the Charter of Fundamental Rights of the EU. The directive needs to be implemented with respect to the principles. Most articles protect the OES rather than the user, especially in areas of accountability and transparency	1
	Penalties	
Preference	Supports enforcement to ensure the protection of human rights. Penalties should be in line with human rights infringements.	
Commission	Art. 17 - member states can lay down their own sanctions and must report them to the Commission once they have been agreed on	1

Parliament	Art. 17 - supports enforcement. Parliament does not mention Human Rights with respect to penalties.	1
Council	Art. 17 - agrees that member states can lay down their own rules. No mention of penalties being in line with human rights.	1
Final	Art. 21 - Member states lay down their own rules to stop infringements. Penalties are effective, proportionate and dissuasive. No mention of protecting human rights as reason for penalties	1
	Actions to be taken by operators	
Preference	Incorporate a capable and secure foundational technology infrastructure. (Access Now, 2019) Decentralized data storage to protect from cyber attacks. (Access Now, 2019)	
Commission	Recital 25 - products do not have to be designed, developed or manufactured in a particular manner.	0
Parliament	Art. 16 - Parliament includes "Member States***, without prescribing the use of any particular technology,*** shall encourage the use of ***European or international interoperable*** standards and/or specifications relevant to networks and information security" No provisions made for decentralised data storage.	0
Council	The Council supports technological neutrality. No provisions made for decentralised data storage.	0
Final	(51) - technology products do not need to be designed, developed or manufactured in a particular manner. Art 19 - forbids discriminination of any type of technology	0
	Risk assessment	
Preference	Assessments should be in line with International Principles on the Application of Human Rights to Communications Surveillance (Access Now, 2015)	
Commission	No mention of human rights in assessing risk.	0
Parliament	No mention of human rights in assessing risk unless it is in relation to personal data. (art. 1) Supports civilian national authorities being involved.	1
Council	Art. 1 - The Council supports notification procedures by OES. Cooperation groups are issued with yearly reports on incidents to monitor the situation. No mention of human rights. However, it is government led.	1
Final	No mention of human rights in assessing risk. However, MS can lay down guidelines for OES to follow. Should	1

	be in line with the principles.	
	Total score Commission	4/16
	Total score Parliament	4/16
	Total score Council	3/16
	Total score final	3/16

Table 33: Preferences for Bits of Freedom (NIS Directive)

	Scope	Score
Preference	Should include government bodies and public administration. All bodies that process personal data should be implicated.	
Commission	Chapter IV - Security of NIS of Public Administration and Market Operators. Not directed at firms that process personal data	1
Parliament	Recital 4a excludes public administration. Limited scope in Annex II & III	0
Council	Annex II does not include public authorities. Includes reservations about adding administrative burdens to startups. They are omitted.	0
Final	Not included as a sector in the annex.	0
	Member state cyber security bureaus	
Preference	Do not establish new authorities. Use resources to invest in staff with relevant expertise and train current staff (BoF, 2012)	
Commission	Art. 7 - supports the establishment of one CSIRT in every member state.	0
Parliament	Art. 7 - supports CERTs. Allows for multiple CERTs but all under the same mandate.	0
Council	Art. 7 - supports the establishment of CSIRTs in every member state.	0
Final	Art. 9 - CSIRTs are established in every MS	0
	Type of incidents to be reported	
Preference	Incidents that infringe personal security need to be reported. This policy should focus on personal security rather than incident reporting All data and security breaches should be recorded on a public registry.	
Commission	Art. 14(2) - incidents which have a significant impact on the security of the core services provided by the operator must be	0

	reported.	
Parliament	Recital 8 - reporting of ***"incident having a significant impact" means an incident affecting the security and continuity of an information network or system that leads to the major disruption of vital economic or societal functions*** " Art. 14a - refers to core services of the provider. Does not increase the scope of incident reporting. Incidents are reported to the authorities. No mention of a public registry.	0
Council	Art. 14(1) & (1a) - incidents related to continuity of essential services need to be reported. Replaces core services with essential. Art. 3a- "essential services" means economic and societal services essential for the functioning of the internal market. Does not support a public registry	0
Final	Art. 14(3) - incidents relating to essential services provided by the OES needs to be reported. Incidents relating to the GDPR fall under a different scope	0
	Accountability of operators of essential services	
Preference	Transparency of OES. Recommends public oversight on this policy (BoF, 2012) Vulnerabilities in information technologies needs to be published as soon possible (BoF, 2012)	
Commission	Art. 14 - The competent authority can require OES to inform the public of incidents if it is deemed to be the best action to take in the public interest. No public oversight in this process.	1
Parliament	No mention of any publishing any vulnerabilities. Recital 28 allows for CERTs to inform firms of vulnerabilities but there is no public accountability. However in Art. 6, the Parliament suggests creating a civilian competent national authority to assist.	1
Council	Art. 14 - The competent authority can require OES to publish incidents relating to specific individuals. However there is no public oversight on this.	0
Final	Art. 14 - incidents are reported to authorities. Authorities have the duty to inform the public when it will help in finding a remedy to the situation. (59) - publishing of incidents will be balanced against protecting the reputation of OES	0

	Direction of cybersecurity	
Preference	Europe and MS must give the right example. MS need additional capacity in the area of ICT, enhancing their own platforms which should not be run by private entities.	
Commission	Art. 16 - The Commission will draw up a set of standards relevant to NIS. The Commission believes that public administration is under the scope of this policy. Stricter measures must be applied. However it does not forbid a public authority in choosing a certain provider.	1
Parliament	Art. 16 - "***without prescribing the use of any particular technology,*** shall encourage the use of ***European or international interoperable*** standards. The parliament does encourage using European standards." 4a - While it mentions that public administrations should protect their own NIS systems, it does not forbid private entities participating.	1
Council	Art. 16 - encourages internationally accepted standards without prejudice to technological neutrality	0
Final	Art. 19 - the directive will not prescribe technological suggestions	0
	Penalties	
Preference	Authorities need to have capacity to determine if cyber incidents create risk to our information security (BoF, 2012) Authorities need to have sufficient budget and power to enforce infringements.	
Commission	Art. 6 - Member states will ensure that competent authorities will have the adequate technical, financial and human resources to carry out their tasks efficiently Art. 17 - member states can lay down their own sanctions and must report them to the Commission once they have been agreed on	2
Parliament	Art. 6 - Member states will ensure that competent authorities and the single point of contact will have the adequate technical, financial and human resources to carry out their tasks efficiently Art. 17(1a) - Member states ensure that OES follows guidelines of directive. Art. 13 - supports international cooperation with third parties.	2
Council	Council removes wording on committing to provide necessary resources for authorities.	0
Final	Art. 8 - MS provides authorities with necessary powers and means to assess the compliance of OES. Art. 15(4) - cooperation with data protection bodies.	2

	Art. 13 - provides scope for international cooperation	
	Actions to be taken by operators	
Preference	Private and public sector firms should invest in diverse IT-systems when buying products and services. Security of systems needs to be improved (BoF, 2012)	
Commission	Recital 25 - OES are not subject to particular products and information tools. They do not have to be designed, developed or manufactured in a particular manner.	0
Parliament	Art. 16 - Parliament includes "Member States***, without prescribing the use of any particular technology,*** shall encourage the use of ***European or international interoperable*** standards and/or specifications relevant to networks and information security"	0
Council	Remains technologically neutral.	0
Final	(51) - technology products do not need to be designed, developed or manufactured in a particular manner. Art 19 - forbids discriminination of any type of technology	0
	Risk assessment	
Preference	Do not depend on third parties on providing information. (BoF, 2012)	
Commission	Entrusts OES in recital 22. However, does support annual reports and cooperation groups to monitor ris. Groups do not involve OES.	1
Parliament	(22) - Supports a close cooperation and trust between OES and authorities. It is a collaborative effort.	0
Council	Art. 1 - The Council supports notification procedures by OES. Cooperation groups are issued with yearly reports on incidents to monitor the situation.	1
Final	(44) - puts the onus on OES to provide information and create an environment of trust.	0
	Total score Commission	6/16
	Total score Parliament	4/16
	Total score Council	1/16
	Total score final	2/16

Table 34: Preferences for EURid (NIS Directive)

	Scope	Score
Preference	"Only business providing or using network and information systems underpinning services which are vital for the functioning	

	of our society, such as transport, energy, finance, health, water and Internet services of general interest (e.g. e-commerce, search engines, social networking).”(EURid, 2012)	
Commission	Annex II - includes similar list of market operators	2
Parliament	Recital 4a - similar outcome “***this Directive should focus on critical infrastructure essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, financial market infrastructures and health.”*** **Omits digital platforms.**	1
Council	All the preferred sectors are included in Annex II by the Council.	2
Final	Similar outcome for Annex II & III	2
	Member state cyber security bureaus	
Preference	No preference	
Commission		
Parliament		
Council		
Final		
	Type of incidents to be reported	
Preference	No defined scope. However, firms should be incentivised to report incidents which appear to have criminal nature. Difficult to objectively define levels of incident reporting (EURid, 2012)	
Commission	Art. 14(2) - incidents which have a significant impact on the security of the core services provided by the operator must be reported.	0
Parliament	The Parliament defines levels of incident reporting in recital 8. Recital 8 - reporting of ***"incident having a significant impact" means an incident affecting the security and continuity of an information network or system that leads to the major disruption of vital economic or societal functions”*** Art. 14a - refers to core services of the provider. Does not increase the scope of incident reporting. Incidents are reported to the authorities.	0
Council	Art. 14(1) & (1a) - incidents related to continuity of essential services need to be reported. Replaces core services with essential. Art. 3a- “essential services” means economic and societal services essential for the functioning of the internal market.	0
Final	Art. 14(3) - incidents relating to essential services provided by	0

	the OES needs to be reported. No incentives exist in this directive.	
	Accountability of operators of essential services	
Preference	The aim should be to increase awareness. It will have a positive global effect on reducing cybersecurity risks. Therefore, public accountability is important.	
Commission	Art. 14 - The competent authority can require OES to inform the public of incidents if it is deemed to be the best action to take in the public interest.	1
Parliament	Art. 14 - limited public accountability.	0
Council	The Council supports increasing awareness. Art. 14 - The competent authority can require OES to publish incidents relating to specific individuals. Supports annual incident reports sent to the cooperation group.	1
Final	Art. 14 - incidents are reported to authorities. Authorities have the duty to inform the public when it will help in finding a remedy to the situation. (59) - publishing of incidents will be balanced against protecting the reputation of OES	0
	Direction of cybersecurity	
Preference	Invest in education. Inform on what risks occur. Involve public-private cooperation mechanisms.	
Commission	Art. 5d - Member states must give an indication of the education, awareness raising and training programmes. Art. 5c - includes cooperation mechanisms between public and private sectors	2
Parliament	Adds text to recital 6. "***Universities and research centres have a decisive role in spurring research, development and innovation in those areas and should be provided with adequate funding.***" Art. 16(2) - The Parliament supports cooperation with relevant stakeholder	2
Council	Art. 16 - encourages participation between ENISA and the member states to create standards.	0
Final	Art. 7(d) - mandates the MS to develop education awareness programmes. Public-private supplementary consultation supports this this partnership (Europa, 2016)	2
	Penalties	
Preference	No legal enforcement but incentives should be provided to those	

	who report incidents. Allow them access to security related fora.	
Commission	The Commission supports legal enforcement	0
Parliament	Parliament supports penalties for non compliance	0
Council	Council supports penalties for non compliance	0
Final	Art. 15 - MS provides authorities with necessary powers and means to assess the compliance of OES. Art. 21 - laws down legal penalties.	0
	Actions to be taken by operators	
Preference	Minimum level of security on infrastructure and procedures. Minimum level of security on all PCs Government needs to improve in infrastructure and procedures.	
Commission	The Commission believes that public administration needs to be under the scope of this directive which would ensure minimum security standards.	2
Parliament	Art. 16 - Parliament includes "Member States***, without prescribing the use of any particular technology,*** shall encourage the use of ***European or international interoperable*** standards and/or specifications relevant to networks and information security"	0
Council	Member states shall ensure that CSIRTs have access to appropriate information infrastructure at national level. However they are not regarded as essential services.	1
Final	(51) - technology products do not need to be designed, developed or manufactured in a particular manner. Art 19 - forbids discriminination of any type of technology	0
	Risk assessment	
Preference	Difficult to empower companies. There is no ultimate effective way to convince firms to invest in security, they want to protect their financial interests as a priority. EU should provide education and guidelines on good practices. (EURid, 2012)	
Commission	Gives greater responsibility to OES in recital 22. Art. 14 - The Commission will provide guidelines.	1
Parliament	(22) - Supports a close cooperation and trust between OES and authorities. It is a collaborative effort. Recital 6 - Parliament calls for more investment in universities to assist in education and research	1
Council	No mention of education. Council does not support convincing firms to invest in security.	1
Final	(44) - puts the onus on OES to provide information and create an	1

	environment of trust. ENISA will work with MS to provide guidelines.	
	Total score Commission	8/14
	Total score Parliament	4/14
	Total score Council	5/14
	Total score final	5/14

Table 35: Preferences for AmCham (NIS Directive)

	Scope	Score
Preference	"The Directive must focus solely on those infrastructures and services which are truly essential to the functioning of a Member State's economy, public health or safety". If they are truly indispensable, they should be covered. Search engines or social media should not be included. (AmCham, 2014)	
Commission	Annex II includes digital infrastructures such as e-commerce, social networks and search engines.	0
Parliament	Deleted all digital platforms - e-commerce, search engines, cloud computing from Annex II.	2
Council	Operators of essential services in specific sectors should be included. SMEs and startups are not included. Includes e-commerce platforms Internet payment gateways Social networks Search engines Cloud computing services. 2013/0027 (COD)	0
Final	Art 5(2) - Services critical to societal and economic activity are covered, (4) - digital service providers should be included. However different rules apply for DSPs	0
	Member state cyber security bureaus	
Preference	Needs to be a harmonisation of requirements across the EU by member states. (AmCham, 2014) This process should be managed by one bureau.	
Commission	Art. 7 - Member states shall set up one CERT in their state. It can be part of a competent authority.	2
Parliament	Changes article 7 to allow for multiple CERTs. Suggests a different CERT for each sector listed in Annex II. However they add wording that the CERT will act as a single point	1

	of contact for a firm.	
Council	Art. 7 - member states can designate one or more CSIRTs. Where there are multiple authorities, the single point of contact and the CSIRT of the same member state shall cooperate closely.	1
Final	Art. 8 - MS assign a single point of contact to manage NIS cooperation of that state. Art. 9 - every member state will establish one or more CSIRTs Art. 12 - CSIRTs will be harmonised in a network across the EU. Art. 18 - DSPs are subject to one CSIRT, where they have their main establishment.	1
	Type of incidents to be reported	
Preference	Truly critical incidents. Very narrow scope. Should be largely voluntary (AmCham, 2013)	
Commission	Art. 14(2) - incidents which have a significant impact on the security of the core services provided by the operator must be reported.	2
Parliament	Recital 8 - reporting of ***"incident having a significant impact" means an incident affecting the security and continuity of an information network or system that leads to the major disruption of vital economic or societal functions"*** Art. 14a - refers to core services of the provider. Does not increase the scope of incident reporting.	2
Council	Art. 14(1) & (1a) - incidents related to continuity of essential services need to be reported. Replaces core services with essential. Art. 3a- "essential services" means economic and societal services essential for the functioning of the internal market.	2
Final	Art 14(3) - incidents that have significant impact on the continuity of essential services they provide need to be reported. Other incidents are not included therefore voluntary.	2
	Accountability of operators of essential services	
Preference	Not to the end customer. They cannot be sure who the actual end user is. Do not put too much pressure on the supplier. Should remain confidential to protect the reputation of the company and the customer. (AmCham, 2014a)	
Commission	Art. 14 - Public administration and market operators will notify competent authorities when incidents occur. The Public will be informed when the competent authority deems it is in the public's best interest. An annual report will be sent to the cooperation group by the competent authorities	0

Parliament	***Recital 28 - "Competent authorities and single points of contact should inform manufacturers and service providers of affected ICT products and services about incidents having a significant impact notified to them"*** Art. 14 (4) - the public may need to be notified if it will assist in solving the incident. However the authorities will protect the name of the market operator concerned	1
Council	Art. 14 - The competent authority can require OES to publish incidents relating to specific individuals. The Council believes that an annual anonymous report should be sent to the Cooperation Group to monitor services.	0
Final	Outcome - in most cases this is fulfilled however there are issues where this will not be the case (see art. 16(7). Art. 14 - incident notifications need to be reported to the competent authority or the CSIRT (whoever the single point of contact is). Art. 16 - refers to incident notifications for DSPs. Art. 16(7) - public can be informed of an incident if it is the only way to prevent the incident.	1
	Direction of cybersecurity	
Preference	Standards put in place should be in line with existing global standards. Europe should stay in line with this. (AmCham, 2014a)	
Commission	Art. 16 - encourages internationally accepted standards without prejudice to technological neutrality.	0
Parliament	Art. 16 - "***without prescribing the use of any particular technology,*** shall encourage the use of ***European or international interoperable*** standards."	2
Council	Art. 16 - encourages internationally accepted standards without prejudice to technological neutrality.	2
Final	Art. 19(1) - promotes internationally accepted standards in promoting NIS. Art. 19(2) - mandates ENISA and MS to draw guidelines of best practice using existing standards as a benchmark and include member states national standards as well if they are different.	2
	Penalties	
Preference	Rules need to be consistent across member states. Penalties should not alter product service or design	
Commission	Art. 17 - sanctions are not standardised. Recital 25 - supports technological neutrality	1
Parliament	Art. 17 - does not standardise penalties across member states.	1

	Recital 25 - supports technological neutrality	
Council	Art. 17 - agrees that member states can lay down their own rules. Supports technological neutrality.	1
Final	Art 21 - penalties must be effective, proportionate and dissuasive. However they are not harmonised across the EU. (51) - technology products do not need to be designed, developed or manufactured in a particular manner.	1
	Actions to be taken by operators	
Preference	Directive should not enforce product or process change of private firms	
Commission	Recital 25 - products do not have to be designed, developed or manufactured in a particular manner.	2
Parliament	Art. 16 - Parliament includes "Member States***, without prescribing the use of any particular technology,*** shall encourage the use of ***European or international interoperable*** standards and/or specifications relevant to networks and information security"	2
Council	Art. 16 - Council promotes technological neutrality.	2
Final	(51) - technology products do not need to be designed, developed or manufactured in a particular manner. Art 19 - forbids discriminination of any type of technology	2
	Risk assessment	
Preference	Self-assessment of private firms as they are most aware of potential risks (AmCham, 2013)	
Commission	(22) Supports a collaborative effort between authorities, member states and stakeholders. Art. 8 - Does not include market operators in the Cooperation Group	1
Parliament	(22) - Supports a close cooperation and trust between OES and authorities. It is a collaborative effort.	2
Council	Art. 1 - The Council supports notification procedures by OES. Cooperation groups are issued with yearly reports on incidents to monitor the situation.	1
Final	(44) responsibilities of ensuring NIS lies with the operators. Risk management and risk assessment needs to be incorporated by the operators. Establish a network of trust between CSIRTs and OES.	2
	Total score Commission	8/16
	Total score Parliament	11/16
	Total score Council	9/16
	Total score final	11/16

Table 36: Preferences for EBF (NIS Directive)

	Scope	Score
Preference	Wide scope. Should encompass any industry that has been subject to cyberattack e.g. hardware and software developers. Legal firms, accountancy firms, SMEs (EBF, 2013).	
Commission	Includes banking industries. Annex II provides a limited scope. Does not include hardware manufacturers and software developers, legal firms etc.	0
Parliament	Includes financial and banking industries. Recital 4a - Hardware manufacturers and software developers should be excluded	0
Council	Does not widen scope to include those mentioned by EBF. However they mention that this is the minimum requirement and encourages MS to add more.	1
Final	(50) - Hardware and software developers are excluded. Scope is not widened from proposal 2013/0027 to final outcome.	0
	Member state cyber security bureaus	
Preference	A designated CSIRT should act as a single point of contact between financial institutions and authorities. (EBF, 2019) CSIRTs should operate in a harmonised network sharing information with each other (EBF, 2019) Create a central reporting hub for all reporting across Europe (EBF, 2019)	
Commission	No mention of single point of contact between CSIRTs and firms. Art. 8 - sets up a cooperation network.	1
Parliament	Art 7(1) - includes wording to create sector specific CERTs. It acts as the single point of contact between financial institutions and authorities. Art. 7(5b) - includes wording "***The CERTs shall be enabled and encouraged to initiate and to participate in joint exercises with other CERTs"***	2
Council	Art. 7 - an entity could have obligations to multiple bureaus. However this will be limited and cohesion is promoted. A cooperation group will be set up.	1
Final	Art. 8(4) - single point of contact acts as a liaison between member states. Art. 12 - CSIRTs will be harmonised in a network across the EU. Strengthening of powers of ENISA as a central EU hub.	2
	Type of incidents to be reported	
Preference	Assign parameters on mandatory incident reporting. Only incidents with significant and material impact should be reported.	

	(EBF, 2013)	
Commission	Art. 14(2) - incidents which have a significant impact on the security of the core services provided by the operator must be reported.	2
Parliament	Recital 8 - reporting of ***"incident having a significant impact" means an incident affecting the security and continuity of an information network or system that leads to the major disruption of vital economic or societal functions"*** Art. 14a - refers to core services of the provider. Does not increase the scope of incident reporting.	2
Council	Art. 14(1) & (1a) - incidents related to continuity of essential services need to be reported. Replaces core services with essential. Art. 3a- "essential services" means economic and societal services essential for the functioning of the internal market.	2
Final	Art. 14 - Only significant incidents are mandatory to be reported	2
	Accountability of operators of essential services	
Preference	Incidents should be reported to authorities. If the public is ever informed, the reputation of the financial firm needs to be protected (EBF, 2013)	
Commission	Art. 14 - Public administration and market operators will notify competent authorities when incidents occur. The Public will be informed when the competent authority deems it is in the public's best interest. An annual report will be sent to the cooperation group by the competent authorities.	0
Parliament	***Recital 28 - "Competent authorities and single points of contact should inform manufacturers and service providers of affected ICT products and services about incidents having a significant impact notified to them."*** Art. 14 - competent authorities are notified. Art. 14 (4) - the public may need to be notified in some circumstances. However the authorities will protect the name of the market operator concerned.	2
Council	Art. 14 - The competent authority can require OES to publish incidents relating to specific individuals. Does not specify whether or not firms should be given anonymity. The Council believes that an annual anonymous report should be sent to the Cooperation Group to monitor services.	0
Final	Art. 14 - incidents are reported to authorities.	2

	(59) - publicity of incidents will be balanced against protecting the reputation of OES	
	Direction of cybersecurity	
Preference	No competence should be given to the EU or member states. Financial industry should come together to create their own guidelines (EBF, 2013)	
Commission	Art. 16 - The Commission will draw up a set of standards relevant to NIS.	0
Parliament	Art. 16 - "***without prescribing the use of any particular technology,*** shall encourage the use of ***European or international interoperable*** standards." Recital 24 - However the Parliament makes special allowances and involvement from the financial industry.	1
Council	Art. 16 - encourages internationally accepted standards without prejudice to technological neutrality. The Council does not support a sector-specific approach.	0
Final	Art. 19(1) - promotes internationally accepted standards in promoting NIS. Art. 19(2) - mandates ENISA and MS to draw guidelines of best practice using existing standards as a benchmark and include member states national standards as well if they are different.	0
	Penalties	
Preference	Enforcement mechanisms should be standardised across Europe. (EBF, 2013)	
Commission	Art. 17 - sanctions are not standardised.	0
Parliament	Art. 17 - does not standardise penalties across member states.	0
Council	Art. 17 - agrees that member states can lay down their own rules.	0
Final	Art. 21 - Member states can lay down their own rules on penalties	0
	Actions to be taken by operators	
Preference	Develop processes in a manner appropriate to their industry, not a one size fits all. Should remain neutral to processes already in place. (EBF, 2013)	
Commission	Recital 25 - products do not have to be designed, developed or manufactured in a particular manner. No sector specific approach.	1
Parliament	Art. 16 - Parliament includes "Member States***, without prescribing the use of any particular technology,*** shall encourage the use of ***European or international interoperable*** standards and/or specifications relevant to networks and information security" Supports sector specific approach.	2

Council	Art. 16 - Council supports technological neutrality. However the Council do not emphasise a sector specific approach compared to the parliament.	1
Final	(51) - technology products do not need to be designed, developed or manufactured in a particular manner. Art 19 - forbids discriminination of any type of technology. However there is no sector-specific approach.	1
	Risk assessment	
Preference	Standards of risk assessment should be created by companies themselves. (EBF, 2013)	
Commission	22) Supports a collaborative effort between authorities, member states and stakeholders. Art. 8 - Does not include market operators in the Cooperation Group	1
Parliament	(44) - risk management is the duty of OES.	2
Council	Art. 1 - The Council supports notification procedures by OES. Cooperation groups are issued with yearly reports on incidents to monitor the situation.	1
Final	(44) - risk management is the duty of OES.	2
	Total score Commission	5/16
	Total score Parliament	11/16
	Total score Council	6/16
	Total score final	9/16

Table 37: Preferences for DigitalEurope (NIS Directive)

	Scope	Score
Preference	"services that are in some sense critical to the functioning of society or the economy should be included. Seeks exclusions for e-commerce platforms, social networks, search engines, app stores or internet payment gateways. Cloud services in some aspects. Other members of information society should be excluded (DE, 2013)	
Commission	Annex II includes all digital operators including e-commerce platforms, social networks, search engines, cloud computing, internet payment gateways, national domain name registries	0
Parliament	Deletes all members of digital society from Annex II	2
Council	Annex II includes all digital operators including e-commerce platforms, social networks, search engines, cloud computing, internet payment gateways, national domain name registries	0
Final	Annex II - includes digital infrastructure.	0

	Annex III - includes online marketplaces, search engines and cloud computing	
	Member state cyber security bureaus	
Preference	Establish a network of CERTs in every member state (DE, 2012a) Cooperation network across every state (DE, 2012a)	
Commission	Art. 7 - Every member state shall set up one CERT in their state. Art. 8 - sets up a cooperation network across the union.	2
Parliament	***Art. 7 (1) - "Each Member State shall set up a at least one Computer Emergency Response Team ("CERT") for each of the sectors listed in Annex II"*** ***(5b) - The CERTs shall be enabled and encouraged to initiate and to participate in joint exercises with other CERTs***	2
Council	Art. 7 - supports a network of CSIRTs in every member state. Art. 8a - establishes a cooperation group. Invites those under the scope of the directive to participate.	2
Final	Art. 9 - every member state will establish one or more CSIRTs Art. 12 - CSIRTs will be harmonised in a network across the EU.	2
	Type of incidents to be reported	
Preference	Incidents relating to the core services of the operator as opposed to incidental services (DE, 2013) Incidents reporting should be limited to those affecting significant impact of essential service (DE, 2012a)	
Commission	Art. 14(2) - incidents which have a significant impact on the security of the core services provided by the operator must be reported.	2
Parliament	Recital 8 - reporting of "***"incident having a significant impact" means an incident affecting the security and continuity of an information network or system that leads to the major disruption of vital economic or societal functions"*** Art. 14a - refers to core services of the provider. Does not increase the scope of incident reporting.	2
Council	Art. 14(1) & (1a) - incidents related to continuity of essential services need to be reported. Replaces core services with essential. Art. 3a- "essential services" means economic and societal services essential for the functioning of the internal market.	2
Final	Art. 14(3) - incidents relating to essential services provided by the OES needs to be reported. Art. 14(3) - incidents that have significant impact to the continuity	2

	of service	
	Accountability of operators of essential services	
Preference	Accountable to the supervisory authority in the MS. (DE, 2012a) Authorities should not have to publicise information about product vulnerabilities prior to appropriate countermeasures being defined and deployed (DE, 2013)	
Commission	Art. 14 - Public administration and market operators will notify competent authorities when incidents occur. The authorities can require the OES to inform the public if it deems it necessary. An annual report will be sent to the cooperation group by the competent authorities.	1
Parliament	Art. 14 - accountable to the single point of contact. It is the contact's duty to alert other affected parties. Supports anonymity of the OES	2
Council	Art. 14 - The competent authority can require OES to publish incidents relating to specific individuals. Does not specify whether or not firms should be given anonymity.	1
Final	Art. 14 - incidents are reported to authorities. (59) - publicity of incidents will be balanced against protecting the reputation of OES	2
	Direction of cybersecurity	
Preference	Address topics through existing global methods (DE, 2013) MS should engage in R&D initiatives on tackling cybercrime (DE, 2012a)	
Commission	Art. 16 - The Commission will draw up a set of standards relevant to NIS.	0
Parliament	Art. 16 - ***without prescribing the use of any particular technology,*** shall encourage the use of ***European or international interoperable*** standards. Art. 8(f) - Includes the role of the European Cybercrime Centre to assist in exchange information on all expertise on European cybercrime matters.	2
Council	Art. 16 - Encourages the use of internationally accepted standards without prejudice to technological neutrality.	2
Final	Art. 7(e) - mandates MS to define their R&D plans relating to NIS Art. 11(f) - facilitates R&D cooperation Art. 19(1) - promotes internationally accepted standards in promoting NIS. Art. 19(2) - mandates ENISA and MS to draw guidelines of best	2

	practice using existing standards as a benchmark and include member states national standards as well if they are different.	
	Penalties	
Preference	If infringement is cross-border, enforcement should be the responsibility of one member state (DE, 2013)	
Commission	In the grounds for the proposal (1.5.1), the Commission considers the cross-border nature of NIS and issues that arise for multinationals. It argues that member states will work together but does not offer a solution to sanctions in multiple member states.0	0
Parliament	Supports enforcement under the single point of contact principle. Later added Art. 18 - Enforcement and jurisdiction.	2
Council	Supports enforcement under the single point of contact principle with respect to non-duplication of procedures.	1
Final	Art. 17(3) - in relation to enforcement, the OES is subject to the authority where its main establishment is located. This is related to DSPs only. DE members fall under this category.	2
	Actions to be taken by operators	
Preference	Specifications from the directive should avoid specific design, development or manufacturing requirements (DE, 2013)	
Commission	Recital 25 - products do not have to be designed, developed or manufactured in a particular manner.	2
Parliament	Art. 16 - Parliament includes "Member States***, without prescribing the use of any particular technology,*** shall encourage the use of ***European or international interoperable*** standards and/or specifications relevant to networks and information security"	2
Council	Art. 16 - Council supports technological neutrality	2
Final	(51) - technology products do not need to be designed, developed or manufactured in a particular manner. Art 19 - forbids discriminination of any type of technology	2
	Risk assessment	
Preference	Competent authorities should require OES to provide necessary information to assess the security of their NIS as opposed to introducing an auditing power (DE, 2013)	
Commission	(22) Supports a collaborative effort between authorities, member states and stakeholders. Art. 8 - Does not include market operators in the Cooperation Group Art. 15(b) - a firm must undergo a security audit carried out by a	0

	qualified independent body or national authority.	
Parliament	(22) - Supports a close cooperation and trust between OES and authorities. It is a collaborative effort. Art. 15(b) - OES must provide evidence of effective implementation of security policies	2
Council	Art. 1 - The Council supports notification procedures carried out by OES to authorities. Cooperation groups are issued with yearly reports on incidents to monitor the situation. Art. 15(b) - Member states shall ensure that the competent authorities have the means to require operators to comply. This can be following a self-assessment from a firm if the state feels further action is required.	1
Final	(44) - Risk assessment is conducted by the OES. Art. 15 - Member states will look for evidence of the effective implementation of security policies.	2
	Total score Commission	7/16
	Total score Parliament	16/16
	Total score Council	9/16
	Total score final	14/16

Table 38: Preferences for European Cockpit Association (NIS Directive)

	Scope	Score
Preference	All businesses that use or provide NIS systems. (ECA, 2012)	
Commission	This directive applies to several sectors who are deemed critical infrastructures of society. No applied elsewhere	0
Parliament	***Rectial 4a - "this Directive should focus on critical infrastructure essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, financial market infrastructures and health"*** ***Omits many providers of NIS systems in Annex II*** ***Includes all air transport related industries.***	0
Council	Council agrees that a greater number of entities concerned with NIS should be included. However for the purposes of harmonisation, they include a minimum list.	1
Final	Annex II & III follows a similar pattern. SMEs and public administration are omitted	1
	Member state cyber security bureaus	

Preference	Recommends establishing a national NIS centre in every MS (ECA, 2012) There should be a platform per sector - specific one for aviation (ECA, 2012)	
Commission	Art. 7 - establishes one CSIRT in every member state. Does not specify sector-specific CSIRTs	1
Parliament	Art. 7 - supports establishing a network of CERTs in every MS. Art. 7 - agrees that CERTs should be sector specific. Every sector mentioned in Annex II will be assigned a CERT. This includes aviation.	2
Council	Art. 7 - supports at least one CSIRT in every member state. Does not support sector specific platforms.	1
Final	Art. 8(1) - each state establishes a competent authority to manage NIS. No sector specific recommendations outlined in directive.	1
	Type of incidents to be reported	
Preference	Incidents caused by poorly designed user interfaces or organisational procedures. (ECA, 2012) Incidents relating to cybercrime (ECA, 2012)	
Commission	Art. 14(2) - incidents which have a significant impact on the security of the core services provided by the operator must be reported.	0
Parliament	Recital 8 - reporting of "***"incident having a significant impact" means an incident affecting the security and continuity of an information network or system that leads to the major disruption of vital economic or societal functions"*** Art. 14a - refers to core services of the provider. Does not increase the scope of incident reporting.	0
Council	Recital 8 - reporting of ***""incident having a significant impact" means an incident affecting the security and continuity of an information network or system that leads to the major disruption of vital economic or societal functions"*** Art. 14a - refers to core services of the provider. Does not increase the scope of incident reporting.	0
Final	Only incidents relating to the essential services of providers are included. Incidental services are omitted. (62) - acknowledges that incidents may be as a result of crime, but does set out mandatory requirements for these incidents to be reported in this directive. Asks MS to encourage OES to report these.	0

	Accountability of operators of essential services	
Preference	Public should not be informed of incidents. The reputation of the sector needs to be protected. This would lead to a distrust of the sector (ECA, 2012) Report to competent authorities.	
Commission	Art. 14 - Public administration and market operators will notify competent authorities when incidents occur. The authorities can require the OES to inform the public if it deems it necessary. An annual report will be sent to the cooperation group by the competent authorities.	1
Parliament	Art. 14 (4) - the public may need to be notified in some circumstances. However the authorities will protect the name of the market operator concerned. The public will only be informed if it will assist in rectifying the incident.	2
Council	Art. 14 - The competent authority can require OES to publish incidents relating to specific individuals. Does not specify whether or not the OES will remain anonymous.	1
Final	Art. 14 - incidents are reported to authorities. (59) - publicity of incidents will be balanced against protecting the reputation of OES	2
	Direction of cybersecurity	
Preference	Should be a cooperation between businesses and authorities to come up with working solutions (ECA, 2012)	
Commission	Commission launched a public-private partnership consultation on how to direct cybersecurity policy in the EU which is attached to this directive (Europa, 2016)	2
Parliament	Art. 16 - "***without prescribing the use of any particular technology,*** shall encourage the use of ***European or international interoperable*** standards." Art. 16(2) The parliament supports consultation with stakeholders in creating standards.	2
Council	Art. 16 - encourages internationally accepted standards without prejudice to technological neutrality. Art. 16(2) - encourages cooperation between ENISA and member states in creating standards.	0
Final	Art. 16 - The Commission will draw up a set of standards relevant to NIS.	0
	Penalties	

Preference	Should be enforced at EU level to ensure a level playing field across the EU (ECA, 2012)	
Commission	Art. 17 - sanctions are not standardised.	0
Parliament	Parliament does not standardise penalties.	0
Council	Art. 17 - agrees that member states can lay down their own rules.	0
Final	Art. 21 - Member states can lay down their own rules on penalties	0
	Actions to be taken by operators	
Preference	Use a certification system to demonstrate compliance of supplier systems, as Apple and Microsoft are developing. A central body should lay down the requirements to be compliant (ECA, 2012)	
Commission	Art. 16 - The Commission mandates itself to write up guidelines. No certification possible,	1
Parliament	Art. 8 - develop, in cooperation with ENISA, guidelines for sector-specific criteria for the notification of significant incidents Ask for a greater role with the European Cybercrime Centre in general.	1
Council	Art. 14 - No mention of certificate possibilities. Ensures that the member states have the means to promote compliance.	0
Final	Art. 14 - ENISA will work with MS to create guidelines for firms to follow to ensure compliance. However there is no central body	1
	Risk assessment	
Preference	Encourage all OES to establish risk management procedures. Impose a general obligation to adopt state of the art measures appropriate to risk. (ECA, 2012)	
Commission	(22) Supports a collaborative effort between authorities, member states and stakeholders. Art. 8 - Does not include market operators in the Cooperation Group	1
Parliament	(22) - Supports a close cooperation and trust between OES and authorities. It is a collaborative effort.	2
Council	Art. 1 - The Council supports notification procedures carried out by OES to authorities. Cooperation groups are issued with yearly reports on incidents to monitor the situation.	1
Final	(44) - risk management is the duty of OES. ENISA and MS to create guidelines.	2
	Total score Commission	4/16
	Total score Parliament	9/16
	Total score Council	4/16

	Total score final	9/16