



BCMUN

British Columbia Model United Nations 2023

Dear Delegates,

My name is Chelsea Lee and I am so grateful to have the opportunity to serve as the Director of the European Union at BCMUN 2023. I am currently in Grade 10 at St. Michaels University School in Victoria, British Columbia, and would love to extend a warm welcome to you all. After discovering Model UN in Grade 7, I have attended numerous conferences, and am so grateful for all the learning and skills they have provided. Inside the committee room, there is an abundance of opportunities to grow and learn, meet new people and gain insight into global issues from different perspectives. I hope that you will find the EU an interesting and enjoyable committee, working with fellow delegates and engaging in fruitful debate. This year, the EU will be discussing a highly essential topic: Regulating the Privacy Policies of Major Technology Companies. Although this topic is expansive and has many complicated problems to unravel, I have confidence in your abilities as delegates to collaborate diplomatically and creatively. I truly encourage all of you to come out of your comfort zones and navigate the topic at hand with resilience and innovation—no matter if BCMUN is your first conference or last. Along with my Chair Erica Lim and my Assistant Director Yuvraj Tejnani, I wish you the best of luck with your conference preparations and I look forward to talking and getting to know all of you. If you have any questions, please do not hesitate to contact me via email. I hope that all of you take away many cherished memories from BCMUN 2023!

Best Wishes,
Chelsea Lee
Director of the EU - BCMUN 2023

Table of Contents

Directors Letter	1
Committee Overview	3
Topic Introduction and History	7
Past Action	9
Current Situation	11
Case Studies	12
Bloc Positions	14
Guiding Questions	17
Further Research	18
Citations	19

Regulating Privacy Policies of Major Tech Companies

Committee Overview

Twenty-seven European nations make up the European Union (EU), an international organization that sets common economic, social, and security policies. The European Union (EU) is a union between 27 European countries that serves as the central platform for the member countries to discuss concerns with the European economy, political relationships, outside threats to the Union, and the well-being of the citizens. Since its formation in 1993, it has enabled the member countries to discuss a variety of topics, such as the issue of climate change, the issue of asylum seekers in Europe, and most recently, the issue of the COVID-19 pandemic. Working diligently, the EU has resolved many crises that threatened the lives of European citizens, formulating economic and political policies and ensuring that justice is brought to those that threaten the peace and stability of Europe. Ultimately, the EU's goal is to achieve sustainable development based on balanced economic growth and offer freedom, security, and justice without internal borders.

Since the creation of the EU, numerous positive highlights have been seen. For instance, when the global financial crisis of 2008 struck, the EU created a series of monetary policies that were used to prevent further decline in the European economy. The policies consisted of 3 main initiatives: first, the European Central Bank (ECB) lowered its main policy interest rate by 325 hundredths, which was considered the lowest since the launch of the euro in 1999, second, increased deposit insurance ceilings, and third, guaranteed bank liabilities and bank recapitalizations to citizens. Furthermore, often regarded as the EU's greatest achievement is the creation of the world's biggest single market, which guarantees the free movement of goods and people, allowing people to work, shop, travel, study and retire anywhere in the EU.

Today, the UN continues its intercontinental influence by conducting annual conferences to discuss various challenges. One challenge, also the topic of the 2023 BCMUN's EU committee, is the issue of regulating the privacy policies of major tech companies.

The EU began a significant expansion into central and eastern Europe in the early twenty-first century after being limited to western Europe at first. The Maastricht Treaty, which went into effect on November 1, 1993, is what established the EU. By establishing a single currency (the euro), a unified foreign and security policy, common citizenship rights, and by advancing cooperation in the areas of immigration, asylum, and judicial affairs, the treaty was intended to improve the political and economic integration of Europe. In recognition of the EU's work to

advance democracy and peace in Europe, the organization received the Nobel Peace Prize in 2012.

Since World War II, numerous attempts to unite Europe have been made, with the EU being one of them. At the end of the war, a number of western European nations sought closer social, political, and economic ties in order to foster France and Germany's long-lasting peace, as well as economic growth and military security. To achieve this, the leaders of six nations—Belgium, France, Italy, Luxembourg, the Netherlands, and West Germany—signed the Treaty of Paris in 1951, creating the European Coal and Steel Community when it went into effect in 1952. The only significant western European nations still outside the EU as of January 1, 1995, were Iceland, Norway, and Switzerland. Sweden, Austria, and Finland also joined the EU at that time. Norway's government made two attempts to join (1972 and 1994), but its citizens rejected each attempt. Early in the 1990s, Switzerland put its application on hold. The European Economic Area, which permits unrestricted movement of goods, services, capital, and people, is made up of Norway, Iceland, and the EU's member states as well as Liechtenstein.

In recognition of social policy as a key element of economic integration, the treaty also established the European Social Fund, which was designed to increase job opportunities by facilitating workers' geographic and occupational mobility. The primary institutions of the EU are the European Community, the Council of Ministers, the European Commission, the European Parliament, the European Court of Justice, and the European Central Bank. A forum for various ministries is the Council of Ministers. Numerous former communist nations in eastern and central Europe submitted applications to the EU following the end of the Cold War.

Their relative lack of economic growth, however, raised concerns that it might prevent them from fully integrating into EU institutions. The EU considered a stratified system to address this issue, whereby certain groups of countries would take part in some aspects of economic integration (such as a free trade area) but not others (e.g., the single currency).. A constitution for the expanded EU is being drafted by the Convention on the Future of Europe, which is led by former French president Valéry Giscard d'Estaing. The distribution of power between large and small members of the EU, as well as how to modify the organization's institutions to accommodate a membership that would be more than four times larger than that of the original EEC, were among the most challenging issues facing the document's authors. Voters in France and the Netherlands rejected the proposed constitution in 2005 because it did not include enough racial and religious language, effectively killing it off—at least temporarily—in the process. The proposed constitution was signed in 2004 but needed to be ratified by all EU members before it could go into effect. A permanent president, a European foreign minister, a public prosecutor, and a charter of fundamental rights would all have been established. The EU would have received a "legal personality" under the proposed constitution, giving it the sole authority to negotiate the majority of treaties on behalf of its members. The powers of the European Parliament would also have been significantly increased. Early in 2007, under German leadership, work on a reform treaty to replace the failed constitution began. As a result, the

Lisbon Treaty, signed in December 2007, required recognition of all 27 EU Member States to enter into force. The treaty, which retained part of the draft constitution, establishes an EU presidency, strengthens the representation of the EU's foreign policy, and gives additional powers to the European Commission, the European Court of Justice, and the European Parliament. In contrast, the Lisbon Treaty amends rather than replaces existing treaties. The treaty collapsed, at least temporarily, in June 2008 after being rejected by Irish voters in a referendum. However, in her second referendum in October 2009, Irish voters overwhelmingly approved the treaty. A week after Ireland's vote, Poland has also completed ratification of the treaty. At that time, the treaty had to be ratified only by one country, the Czech Republic. The Czech parliament had already approved the treaty, but Czech President Vaclav Klaus refused to sign it, expressing concern that it threatened Czech sovereignty. After the Czech Constitutional Court ruled in early November that the treaty did not jeopardize the Czech constitution, Klaus reluctantly approved the document and completed the country's ratification process. After approval by all 27 Member States, the Convention entered into force on December 1, 2001.

Topic Introduction and History

One of the first notable notions of the Right to Privacy was part of the 1950 European Convention on Human Rights, which stated that “everyone has the right to respect for his private and family life, his home and his correspondence.” From this basis, the European Union has sought to ensure the protection of this right through legislation. However, with the passing of time and the emergence of the digital age, the EU recognized the need for modifications of the original notion.

The first major step towards regulating data privacy was the creation of Directive 95/46/EC (or just known as “The Directive”) in 1995, a reference text at the European level on the protection of personal data. The paper established minimum data privacy and security standards and the principles of data quality, which stated, for all lawful data processing activities, that personal data must be processed fairly and lawfully, and collected for specified, explicit and legitimate purposes and forbade process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. The paper aimed to establish a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the EU and set up a regulatory framework that sought to accomplish such a goal.

While the directive had a great influence on data privacy in the 1990s, with the creation of new technologies, it slowly began to become obsolete. In 2000, a majority of financial institutions offered online banking. In 2006, Facebook opened to the public, and in 2011, a Google user sued the company for scanning her emails, and with the rapid increase of tech giant companies in Europe such as Trivago and Rovio, EU policymakers were forced to design flexible privacy and data protection laws in the hopes of regulating big internet technology companies. In 2011, Europe's data protection authority declared the EU needed “a comprehensive approach on personal data protection” and work began to update the 1995 directive. The Directive was repealed with effect in the year 2018, as the processing of data became ubiquitous and a new act was needed in order to take modern technology into account.

In the place of Directive 95/46/EC came the General Data Protection Regulation, or GDPR, which was adopted in 2016 and came into effect across all EU members immediately after the repealing of the Directive in 2018. GDPR had a dramatic impact on the EU because unlike directives, where it only lays down certain results that must be achieved but gives each Member State freedom to decide how to transpose directives into national laws, GDPR, a regulation, bound legal force throughout every Member State to enter the principles set in the GDPR to come into force on a set date. The GDPR offered three enhancements into data privacy. First, the regulation had a wider scope and applied to other countries even if they were not in the EU—according to Article 3 in the GDPR’s territorial scope, if they processed personal data, offered goods or services of any kind to EU citizens or residents, they had to adhere to the regulation. Second, the fines for violation of data privacy increased significantly, demanding as high as €20 million, or 4% of global revenue. Third, define an array of legal terms at length. Unlike previous policies, it thoroughly defines many important concepts of privacy, including personal data, data processing, and the data subject.

Today, the GDPR continues to remain in effect. However, despite its accomplishments, GDPR has numerous limitations and loopholes. For instance, in 2018, None Of Your Business (NOYB) filed a complaint under the GDPR, alleging Google, Whatsapp, Facebook, and Instagram for forcing people into giving up their data without obtaining proper consent. Four years later, NOYB is still waiting for final decisions to be made, and this is only of the many cases existing. Data regulators tasked with enforcing the law have struggled to act quickly on complaints against big tech firms and the murky online advertising industry, with scores of cases still outstanding. As a result, civil society groups have grown frustrated with GDPR’s limitations, and while they complain the system to handle international complaints is bloated and slows down enforcement, by comparison, the information economy moves at a significantly faster rate. The slow speed of the system leaves loopholes for data brokers, businesses that collect personal information about consumers and sell that information to other organizations, and abuses in the online advertising industry. Thus, more modifications are needed in order to fully resolve the problem of regulation policies for technology companies.

Past Action

In the twentieth and post the twentieth century the European Subcontinent witnessed many geopolitical, technological and economic changes with the dissolution of the Soviet Union and culmination of the Cold War , an advancement in the technological fields with many new startups that are industrialized tycoons in today's world such as LuKOil , Fortrum , Gazprom Neft , The AXA Group and the recent Stellantis Group , these companies have shaped the economy and well-being of Europe's developed and developing nations such as Finland , Netherlands and France . In recent years many major tycoons have been in cases of theft such as the Red Cross Data Breach , an international emergency including an international organization in an external private Swiss company , the European Union have gotten stricter with their actions , data breaches were prominent in Europe as of the 1980s therefore an act and bill was passed by the European Commission , A directive (Directive 95/46/EC) adopted by the European Commission in 1995 established the groundwork for data protection legislation in the EU. The processing of personal data about persons, including its collection, use, storage, disclosure, and destruction, was governed by the directive. The directive was independently enacted into national law by each of the 27 EU member states and the nations of the European Economic Area (which includes Norway, Iceland, and Liechtenstein). Data protection rules and regulations differed slightly between nations as a result of the directive's provisions being implemented separately by each nation. Post 1995 there have been many conferences and actions taken by the European Union such as the one in 2012 , that included the enhanced reformation and amendment to the 1995 EU Data Act during the Brussels Conference , to strengthen online privacy rights and advance Europe's digital economy, the European Commission had suggested a thorough revision of the EU's 1995 data protection laws. Our data collection, access, and use have all undergone significant changes as a result of technological advancement and globalization. There were also differences in how the 1995 regulations were applied by the 27 EU Member States, which led to enforcement disparities. With the existing fragmentation and high administrative costs eliminated by a single statute, firms will save about €2.3 billion annually. The project contributed to bolstering consumer trust in online services, giving growth, employment, and innovation in Europe a much-needed boost. Other than that in 2012 , the WP29 act was passed by the EU further enhancing data protection and economic efficiency post the Global Economic Crisis of 2008 , in the brief the Article 29 of the Working Party laws suggest that Organizations are required to notify their data protection authority of data breaches within 72 hours, unless the incident is unlikely to put people at danger. They will need to notify the people who are affected in certain circumstances.

Current Situation

The EU is actively trying to look forward concerning the privacy policies of technology companies and has started with a comprehensive new data privacy rule that has been agreed upon by European legislators. This is just one of several recent measures that have been considered in international markets and could have an impact on U.S. Education Technology (Ed-Tech) companies. The Digital Markets Act and the Digital Services Act, both of which were approved by the European Commission last month, aim to protect the rights of internet users, filter out harmful and illegal content, increase platform transparency, and outlaw targeted advertising to children. Another policy is the EU General Data Protection Regulation (GDPR), which went into effect on May 25, 2018, governing how the personal data of EU citizens may be processed and transferred. GDPR is a comprehensive privacy law that applies to all industries and businesses of all sizes. It is intended to replace the 1995 Data Protection Directive. The overall goals of the measures are the same: to establish rules for the protection of personal data and data movement. After this policy was passed, Abriela Zanfir-Fortuna, vice president of global policy at the Future of Privacy Forum (a Washington-based data privacy advocacy organization), said she has noticed a much greater focus on protecting data privacy internationally. The broad law placed restrictions on the data-gathering and processing practices of businesses. Additionally, in 2021, the EU Court of Justice concluded that big tech companies like Facebook, Google, and Twitter can be challenged on data and privacy and sued under certain conditions by any data protection authority in the European Union. The decision clarifies the GDPR's stringent privacy rules and has huge privacy implications for all big tech companies that operate in the European Union, as well as smaller businesses. The European Consumers' Organisation (BEUC) has welcomed the verdict, which they say will help better protect consumers' personal data.

Case Studies

1. Hungary

The current issue of data privacy in Hungary has been a persistent problem for the past several years. According to a study done in May 2021 regarding various elements such as cybercrime and data protection, Hungary was ranked the lowest out of all of the EU countries, with only 13% of its companies enforcing data protection strategies.

Hungary is subject to Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (the “Data Protection Act”), which was amended in 2018 to implement the changes of the GDPR, and in addition also adopted the GDPR Omnibus Act in 2019 in an attempt to modernise consumer protection legislation and strengthen their enforceability. However, while such modifications are effective in preventing individuals from breaching data security, data privacy remains as a constant struggle, as exploitation of user information is rampant in the country, with the federal government being caught for misuse of personal data during the 2022 national elections campaign while attempting to shift the citizens’ favors towards the ruling party, Fidesz.

2. Germany

During recent years, Germany has been wary of US tech giants, specifically “The Big Four,” consisting of Google, Apple, Amazon and Facebook. As a result, the Federal Cartel Office of Germany, responsible for regulating the German market economy, opened proceedings against the Big Four through their 2021 Act against Restraints of Competition (GWB amendment), which aims to or penalize the anti-competitive practices of powerful companies, such as exploiting and selling private user data.

3. France

France has openly shown its ambitions by pushing for many previous European Union reforms, such as the Digital Services Act (DSA), to tackle the issues of data privacy, online hate speech, and misinformation. France also has the French Data Protection Act, which covers both personal and sensitive technological data. Unless there is some exception such as a legal case, France's internal security, or the life of a human at stake, all data handlers, public and private, are supposed to adhere precisely to the law's requirements.

Bloc Positions

Keeping in mind that there is a clear consensus that privacy policies for major technology companies are extremely important, the view on the severity of these policies and measures differs from bloc to bloc, with different opinions surrounding privacy and individual countries' digital policies.

Extreme Technology Privacy Policy Stance

The thought that major technology companies' privacy policies must be managed with strict rules and regulations is shared by Germany, Italy and France. Previously, Germany has made clear statements about their stance through a recent reformation of technology rules. As the EU's economic and political powerhouse, Germany will play a crucial role in debate, pushing for extreme and strict privacy policies against the major technology companies such as Facebook, Google and Twitter. Clemens Otte, senior manager for digitalization with the Federation of German Industries (BDI), argued during a Global Policy Lab's conference in 2017 that Germany's strict data protection laws may be standing in the way of the country's ability to seize digital opportunities. In March 2021, the Chancellor of Germany, along with Denmark's, Finland's, and Estonia's leaders, sent a letter to the EU serving as a dire warning on the dangerous influence of major technology companies. This letter recognizes the EU's reliance on these companies, stating, "At the same time, the dependencies and shortcomings in European digital capacities, skills and technologies have become more apparent."

France and Italy are also significant countries in this bloc. The Italian Data Protection Authority (Garante per la protezione dei dati personali) is an independent authority set up to protect fundamental rights and freedoms in connection with the processing of personal data, and to ensure respect for individuals' dignity. In addition, in late 2020, Italy oversaw many harsh actions against major technology companies, fining and attacking Amazon, Google, Facebook and others for abuse of their dominant positions and antitrust. France has openly shown its ambitions by pushing for many previous European Union reforms, such as the Digital Services Act (DSA), to tackle the issues of data privacy, online hate speech, and misinformation. Policies this bloc may support include increased privacy policy regulation, strict enforcement of penalties after violations, and fining higher sums of money. Higher fines may be an advantageous option, as major technology companies generate so much revenue that current fines do not affect them in an extreme way. This bloc may also support government intervention, and may have interest in a Digital Services Tax (DST), as it would charge technology companies for the transmission of data collected about users for advertising purposes, and may incentivise companies from doing so. France has expressed plans to reform content moderation bills so that it would not need to be reliant on other countries' regulators to enforce and punish larger platforms when they stray from

their privacy policies. The Netherlands and Belgium have also voiced their opinions in the DMA, favouring stricter and heavier protection regulations. Within the EU, the Dutch government has advocated for regulation for big platforms with a gatekeeper role. They also have stated multiple times that they take a positive view of other measures that increase data protection levels.

Moderate Technology Privacy Policy Regulation

Many countries in the EU hold a neutral stance and do not necessarily support severe technology privacy policies. A strong majority of the EU supports the DMA and DSA, but most countries, such as Finland and Portugal, have other priorities or have yet to fully address the situation. Unlike Germany, Italy, and France, this bloc would be satisfied with the implementation of the DSA and DMA, arguing that more extreme policies (such as a DST) would incentivize bigger technology companies to not sell products in the EU, which would be detrimental to the economy. However, for the future, this bloc would support media literacy as a way to educate citizens to protect their own data and privacy online, especially as this solution does not create more tension with the big technology companies. Furthermore, encouraging newer companies with tighter data privacy standards would set the figurative privacy policy bar higher for the major technology organizations, and would force them to compete. This is not out of the question, but would require resources and time. As an example, Greece has more urgent issues, including its environment and economical challenges, that make funding resources into new technology companies not a serious concern. Essentially, the majority of countries within the EU would have a moderate technology regulation approach through solutions such as the implementation of the DSA and DMA and media literacy instead of supporting the more extreme regulations that the previous bloc agrees with.

Anti-Technology Privacy Policy Regulation

Some countries believe that major technology companies should be more lenient with privacy policies, and that the market should have little government intervention. More right-leaning countries such as Austria, Hungary, and Poland tend to minimize privacy regulations on businesses, reduce government spending on policy enforcement and introduce clauses that are applicable to all businesses, not only the technological ones. After initially following Germany in banning Google Street View to protect its citizens' privacy, Austria reversed its decision in 2018. Delegates of this bloc may support more relaxed policies, including individual freedom to study media literacy, with a focus into cybersecurity and privacy protecting measures. Their belief is more that it is up to the citizens to protect themselves and make their own choices. By believing that privacy breaches are somewhat inevitable in market economics, there is no need for preventive policies with governmental interference. Instead, justification for punishment only occurs when influential tech companies abuse their procedures. Due to individual freedom being a large focal point for this bloc, delegates may look towards consequences for digital platforms in a circumstance by circumstance basis, instead of one broad

punishment rule. Countries in this bloc would cautiously support the DSA, so long as its enactments do not impede on politics or freedom of speech. Unlike Ireland, the Netherlands, and Luxemburg, countries in this bloc would support the large-scale implementation of a DST, as most already have one. On a separate note, Ireland shares this bloc's regard in the DMA but not the DSA. In fact, Ireland claims that the DMA and DSA restrict innovation in the European Union. Ultimately, this bloc champions freedom of speech, and therefore minimal privacy - if chosen - and minimal government interference, preferring instead to limit their intervention in the major technology companies.

Guiding Questions

1. What economic incentives are there either in place or pending adoption to pursue digital safety in your country/bloc?
2. What is the consensus from your country's citizens towards being a member of the EU and/or the technology regulations adopted in your country?
3. What is your country/bloc doing to address Europe's so-called "technology gap"?
4. How has the Russian invasion of Ukraine affected your country's technological infrastructure and development plans?
5. What are your country's views on privacy policies? Is there more privacy needed, or is it beneficial to be more open and shared?
6. What is your country/bloc's view on the GDPR? Are there any political or societal tensions due to the GDPR?
7. What roles do free speech, media literacy, and content moderation play in the EU data privacy debate?

Further Research

<https://gdpr.eu/>

Provides a comprehensive overview of the GDPR, its goals, current policies in effect relating to the GDPR, and many more.

https://edps.europa.eu/system/files/2022-04/2022-04-20-edps_annual_report_2021_en.pdf

Chapter 5 of the annual 2021 from the European Data Protection Supervisor (EDPS) provides an in-depth review of the EU's past and future actions regarding data privacy.

https://uploads-ssl.webflow.com/5eb02b586a75d02e7a344a20/60f6777f53166640a9ba462d_EN_Methodology%20Dataprotection%20Ranking.pdf

The report provides a concise overview of how effective each country's data protection policies have been, from government enforcement of data privacy laws to data breach policies in companies to the percentage of malware in the citizens' electronic devices.

<https://www.theregreview.org/2022/03/12/saturday-seminar-data-privacy-through-lens-big-tech/>

This article provides a list of research reports done by accredited professors and/or organizations that contain a variety of relevant information such as the methodology behind sharing consumer data with third parties, flaws in the GDPR, and data privacy policies enforced in countries outside the EU that could potentially serve as additional guides when drafting resolutions.

https://lewisbrisbois.com/assets/uploads/files/GDPR,_Part_I-_History_of_European_Data_Protection_Law.pdf

This report provides a detailed timeline of past actions taken by the EU to manage data privacy. The timeline starts from 1995, at the start of the digital age to year 2016, when the GDPR was adopted.

Citations

1. *General Data Protection Regulation (GDPR) Compliance Guidelines*, <https://gdpr.eu/>. Accessed 22 December 2022.
2. “Addressing the European technology gap.” *McKinsey*, 22 September 2022, <https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/securing-europe-s-competitiveness-addressing-its-technology-gap>. Accessed 22 December 2022.
3. “Big tech companies exposed to EU privacy cases after court decision.” *Euronews*, 15 June 2021, <https://www.euronews.com/2021/06/15/big-tech-companies-exposed-to-privacy-challenges-after-eu-court-decision>. Accessed 11 December 2022.
4. Burgess, Matt. “How GDPR Is Failing | WIRED UK.” *Wired UK*, 23 May 2022, <https://www.wired.co.uk/article/gdpr-2022>. Accessed 22 December 2022.
5. “Countries in the EU and EEA.” *GOV.UK*, <https://www.gov.uk/eu-eea>. Accessed 15 December 2022.
6. “Data protection and online privacy - Your Europe.” *European Union*, 7 January 2022, https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm. Accessed 15 December 2022.

7. “Data Protection Laws and Regulations Report 2022 The Rapid Evolution of Data Protection Laws.” *ICLG*,
<https://iclg.com/practice-areas/data-protection-laws-and-regulations/1-the-rapid-evolution-of-data-protection-laws>. Accessed 22 December 2022.
8. “Difference between a Regulation, Directive and Decision - United States Mission to the European Union.” *USDA-eu.org*, 13 April 2022,
<https://www.usda-eu.org/eu-basics-questions/difference-between-a-regulation-directive-and-decision/>. Accessed 22 December 2022.
9. “EUR-Lex - 31995L0046 - EN.” *EUR-Lex*,
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML_L. Accessed 15 December 2022.
10. “EUR-Lex - I14012 - EN.” *EUR-Lex*, 8 March 2014,
<https://eur-lex.europa.eu/EN/legal-content/summary/protection-of-personal-data.html>. Accessed 22 December 2022.
11. “European Union - Data Privacy and Protection.” *Privacy Shield*,
<https://www.privacyshield.gov/article?id=European-Union-Data-Privatization-and-Protection>. Accessed 15 December 2022.
12. “European Union gateway.” *European Union*,
https://european-union.europa.eu/index_en. Accessed 15 December 2022.
13. “The History of the General Data Protection Regulation.” *European Data Protection Supervisor*,
https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en. Accessed 20 December 2022.
14. “Meet Europe's tech giants | World Economic Forum.” *The World Economic Forum*, 6 October 2017, <https://www.weforum.org/agenda/2017/10/meet-europe-top-tech-titans/>. Accessed 22 December 2022.
15. “New European Data-Privacy Policy Carries Implications for Ed-Tech Companies - Market Brief.” *EdWeek Market Brief*, 23 May 2022,
<https://marketbrief.edweek.org/marketplace-k-12/new-european-data-privacy-policy-carries-implications-ed-tech-companies/>. Accessed 15 December 2022.
16. “Privacy Policy.” *HelpGuide.org*, <https://www.helpguide.org/privacy-policy.htm> . Accessed 15 December 2022.
17. “VMUN 2023 European Union Background Guide.” *VMUN-2023-EU*,
[file:///C:/Users/chels/Downloads/VMUN-2023-EU%20\(1\).pdf](file:///C:/Users/chels/Downloads/VMUN-2023-EU%20(1).pdf). Accessed 23 December 2022.
18. “A third of EU countries oppose changing bloc's treaties.” *EURACTIV.com*, 9 May 2022,
<https://www.euractiv.com/section/future-eu/news/a-third-of-eu-countries-oppose-changing-blocs-treaties/> . Accessed 23 December 2022.
19. Belson, Rosemary. “German industry: Strict privacy laws hinder innovation.” *POLITICO*, 26 September 2017,

- <https://www.politico.eu/article/german-industry-strict-privacy-laws-hinder-innovation/> . Accessed 25 December 2022.
20. “Italy - New Data Protection Overview | Guidance Note.” *DataGuidance*, <https://www.dataguidance.com/notes/italy-data-protection-overview> . Accessed 25 December 2022.
21. “Dutch position on the proposal for the Digital Markets Act.” *The Netherlands at International Organisations*, 17 February 2021, <https://www.permanentrepresentations.nl/documents/publications/2021/02/17/dutch-position-on-the-proposal-for-the-digital-markets-act> . Accessed 25 December 2022.
22. “Digital Services Tax Act.” *Canada.ca*, 14 February 2022, <https://www.canada.ca/en/department-finance/news/2021/12/digital-services-tax-act.html> . Accessed 26 December 2022.
23. Asen, Elke, and Daniel Bunn. “Digital Tax Update: Digital Services Taxes in Europe.” *Tax Foundation*, 22 November 2021, <https://taxfoundation.org/digital-tax-europe-2020/> . Accessed 26 December 2022.
24. “France Data Protection Act: Overview - Securiti.” *SECURITI.ai*, <https://securiti.ai/france-data-protection-act/> . Accessed 1 January 2023.