Legal Issues in Reconciling Data Protection, AI, and Cybersecurity under EU Law

*Iain Nash, DeBrae Kennedy-Mayo, Peter Swire, and Annie Antón**

ABSTRACT

This Paper focuses on certain legal responsibilities under European Union ("EU") law for companies that provide cybersecurity services, by examining the intersection of data protection (privacy), cybersecurity, and artificial intelligence ("AI"). This Paper explores these issues in the context of a hypothetical cybersecurity company known as "ACME Cyber Sentinel" providing services to a hypothetical client named "TechGuard." In four scenarios, this Paper explores ACME Cyber Sentinel: (1) providing cybersecurity service to TechGuard; (2) gathering and processing data from multiple clients to analyze potential cybersecurity threats; (3) training, evaluating, and deploying AI cybersecurity tools; and (4) using these AI cybersecurity tools to provide the cybersecurity services to TechGuard. Each of these scenarios includes two variations. The first variation examines when the two companies are both based in the EU, with no processing taking place outside the EU; the second variation envisions that ACME Cyber Sentinel is based outside of the EU, so that data flows to a different jurisdiction. This Paper also analyzes legal principles from the EU General Data Protection

*Iain Nash is Senior Lecturer in Artificial Intelligence and Technology Law, School of Law and Criminal Justice, Edge Hill University. DeBrae Kennedy-Mayo is Faculty in Law & Ethics in the Georgia Institute of Technology Scheller College of Business and a Senior Fellow, the Cross-Border Data Forum. Peter Swire is the J.Z. Liang Chair in the Georgia Institute of Technology School of Cybersecurity and Privacy, and Professor of Law & Ethics, Georgia Tech Scheller College of Business. He is Research Director of the Cross-Border Data Forum and senior counsel with Alston & Bird LLP. Dr. Annie I. Antón is a Professor in (and former chair of) the School of Interactive Computing at the Georgia Institute of Technology. The authors have no conflicts to report. The authors wish to thank Christoph Bausewein, Kyle Diep, Jake Gord, Emily Hancock, Sam Kaplan, Nathan Lemay, Audheya Mannepalli, Dan Nelson, and Hal Overman. The authors would like to thank participants at a conference hosted by the Cross-Border Data Forum and the Cybersecurity Coalition for their helpful comments.

Regulation ("GDPR")[1] and EU regulation establishing harmonized rules on AI ("EU AI Act")[2] in the context of the main purposes for which cybersecurity companies use personal data—to provide cybersecurity services to protect the personal data of the client company and to maintain state-of-the-art cybersecurity services and tools (such as identifying new cybersecurity threats or training the algorithms used in these cybersecurity tools). This Paper concludes with the finding that EU-based businesses can enter into contracts with cybersecurity companies to protect EU data with state-of-the-art cybersecurity services and tools, but it is more difficult to locate a lawful basis for using EU data to identify new cybersecurity threats or to train new machine learning, AI and other cybersecurity tools. To conclude, it is clear that further clarification from EU decision-makers would help define whether and how access to personal data will be lawful for cybersecurity purposes.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) 2016 O.J. (L. 119) 1, 110 [hereinafter GDPR].

[2] Regulation (EU) 2024/1689 of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence and Amending Certain Union Legislative Acts [hereinafter EU AI Act].

TABLE OF CONTENTS

I. INTRODUCTION

This Paper examines the intersection of data protection (privacy), cybersecurity, and artificial intelligence ("AI") under European Union ("EU") law. It focuses on certain legal responsibilities of companies that provide cybersecurity services related to privacy and AI. For ease of reading, this Paper talks of a hypothetical cybersecurity company known as "ACME Cyber Sentinel" providing services to a hypothetical client named "TechGuard." In four scenarios, this Paper explores ACME Cyber Sentinel: (1) providing cybersecurity service to TechGuard; (2) gathering and processing data from multiple clients to analyze potential cybersecurity threats; (3) training, evaluating, and deploying AI cybersecurity tools; and (4) using these AI cybersecurity tools to provide the cybersecurity services to TechGuard. Each of these scenarios includes two variations. The first variation is when two companies are both based in the EU, with no processing taking place outside the EU, providing 24/7 service using a "follow-the-sun" strategy for staffing service activities;[3] the second variation envisions that ACME Cyber Sentinel is based outside of the EU, so that data flows to a different jurisdiction.

This Paper also analyzes legal principles from the EU General Data Protection Regulation ("GDPR") and EU regulation establishing harmonized rules on AI ("EU AI Act").[4] The authors examine EU law and regulations for several reasons. First, many countries have enacted data privacy laws based on the EU's GDPR, and in many respects the EU's legal regime is the most fully articulated by case law and secondary legislation.[5] The second reason is the significant population and economy of the EU.

---

[3] "The traditional 'follow-the-sun' model is a type of global workflow in which issues can be handled by and passed between offices in different time zones, increasing responsiveness and reducing delays." Tara Ramroop, *What is the Follow-the-Sun Model? Advantages + Strategy*, ZENDESK (Dec. 7, 2023), https://www.zendesk.com/blog/improve-remote-support-follow-sun-model/ [https://perma.cc/H6DE-JBQZ]; *see* Nataliya Andreychuk, *Follow-the-Sun Model: How to Overcome Challenges and Discover Opportunities*, FORBES (Dec. 5, 2022, 7:30 AM), https://www.forbes.com/sites/forbesagencycouncil/2022/12/05/follow-the-sun-model-how-to-overcome-challenges-and-discover-new-opportunities/ [https://perma.cc/5ZGK-LZDK].

[4] GDPR, *supra* note 1; EU AI Act, *supra* note 2. The authors have chosen to analyze the implication of the EU's GDPR and the EU AI Act. Many other EU legal requirements could impact these scenarios, including the Data Act, the Digital Services Act, and the Network and Information Security 2 Directive ("NIS2 Directive"). *See* Isabella Roccia, et al., *European Strategy for Data – Overview of New Regulations*, IAPP (July 2024), https://iapp.org/resources/article/european-strategy-for-data-overview-of-new-regulations/ [https://perma.cc/RM4L-UVEV].

[5] For previous analysis by co-authors Kennedy-Mayo and Swire, see Peter Swire et al., *Risks to Cybersecurity from Data Localization, Organized by Techniques, Tactics, and Procedures*, J. CYBER POL'Y, Aug. 2024, at 1, 2 [hereinafter *Techniques, Tactics, and Procedures*]; *see also* Peter Swire & DeBrae Kennedy-Mayo, *The Effects of Data Localization on Cybersecurity – Organizational Effects*, ARIZ. L.J. EMERGING TECH. (forthcoming 2024) [hereinafter *Organizational Effects*].

This Paper concludes with two main takeaways after examining the main purposes for which cybersecurity companies use personal data—to provide cybersecurity services to protect the personal data of the client company and to maintain state-of-the-art cybersecurity services and tools (such as identifying new cybersecurity threats or training the algorithms used in these cybersecurity tools). The first takeaway is that cybersecurity companies, EU-based or non-EU-based, can provide many cybersecurity services to EU-based businesses, and these services likely can include AI cybersecurity tools. Importantly for most non-EU-based cybersecurity companies, additional protections are needed to address the legal concerns around personal data "transfers." The second takeaway is cautionary; the legal protections for personal data in the EU may make it difficult for cybersecurity companies to utilize this data to update state-of-the-art cybersecurity services and tools. In essence, EU-based businesses can enter into contracts with cybersecurity companies to protect EU data with state-of-the-art cybersecurity services and tools. However, it is more difficult to locate a lawful basis for using EU data to identify new cybersecurity threats or to train new machine learning, AI and other cybersecurity tools.

II. SCENARIOS

This Paper begins by presenting four scenarios involving ACME Cyber Sentinel, a hypothetical cybersecurity company, and TechGuard, a hypothetical EU-based business with all data processing taking place solely in the EU. In these scenarios, this Paper explores ACME Cyber Sentinel (1) providing cybersecurity services to TechGuard; (2) collecting a limited amount of data from ten clients, including TechGuard, to assess potential cybersecurity threats; (3) using the data collected from the ten clients for training, evaluating, and deploying AI cybersecurity tools; and (4) utilizing these state-of-the-art AI cybersecurity tools when providing cybersecurity services to TechGuard.

In these scenarios, machine learning ("ML") is an important subset of AI. ML "allows machines to extract knowledge from data and learn from it autonomously."[6] ML in cybersecurity can detect malicious payloads and behaviors to prevent an adversary from achieving their objective. Such adversarial objectives may be, for example, either criminal (such as a ransomware actor or access broker) or a nation state with goals varying from espionage to sabotage. In such conflicts, it is important to recognize several important facts.[7] Specifically, ML training is necessary for detecting known malware, but it is also capable of preventing unknown or zero-day malware.

---

[6] *Artificial Intelligence (AI) vs. Machine Learning (ML)*, GOOGLE CLOUD, https://cloud.google.com/learn/artificial-intelligence-vs-machine-learning# [https://perma.cc/2HHW-RUNR] (last visited Aug. 22, 2024).

[7] Sven Krasser et al., *Machine Learning-Based Malware Detection in a Production Setting*, *in* MALWARE: HANDBOOK OF PREVENTION AND DETECTION (Dimitris Gritzalis et al. eds, forthcoming 2024).

ML can identify malicious intent based solely on the attributes of a file—without prior knowledge of it, without signatures, and without needing to execute the file to observe its behavior. When well-designed, ML can be an effective weapon against malware. However, no one should rely on ML alone to protect endpoints. It is more effective to implement a comprehensive endpoint security solution that includes ML but is integrated with complementary technologies, such as exploit prevention and behavioral analysis. This alternative increases the ability to protect against a wide range of attacks, whether malware is used or not.[8]

ML enables a more proactive posture than traditional cybersecurity methodologies, including signatures and heuristics. ML offers defensive advantages such as detecting and reacting to an attack in real-time (without the need for a signature update) and identifying attack patterns to predict malware behavior. Cyberattacks from both criminal elements and state-sponsored groups are on the rise, while organizations also struggle with a global cybersecurity workforce shortage.[9] Within this context, ML can augment human analysts and automate repetitive tasks, freeing up analyst time. ML thus represents an important solution to major challenges facing the cybersecurity industry.[10] Due to the importance of ML as a subset of AI, the scenarios discussed here address the legal status of ML and other varieties of AI for achieving overall cybersecurity goals, consistent with other EU legal requirements, including data protection.

A. Scenario 1 – ACME Cyber Sentinel and TechGuard enter into an agreement for AMCE Cyber Sentinel to provide Cybersecurity Software as a Service ("CSaaS")

TechGuard, an EU-based technology company,[11] contracts with ACME Cyber Sentinel to implement a CSaaS solution.[12] ACME Cyber Sentinel is

---

[8] *See* Sven Krasser, *Why Machine Learning Is a Critical Defense Against Malware*, CROWDSTRIKE (July 17, 2019), https://www.crowdstrike.com/blog/defending-against-malware-with-machine-learning/ [https://perma.cc/25Z2-UWQ9].

[9] "In today's hyperconnected digital landscape, the cybersecurity industry faces a critical global shortage of nearly 4 million professionals." MARIE LAURE ESI ALORVOR & NATASA PERUCICA, STRATEGIC CYBERSECURITY TALENT FRAMEWORK WHITE PAPER 3 (World Economic Forum ed., 2024).

[10] Krasser et. al, *supra* note 7.

[11] The EU-based company in this scenario can be considered to operate only in the EU. One can certainly imagine an EU-based company, such as Volkswagen, that is based in the EU but operates globally. Numerous issues arise with an EU-based company that operates globally dealing with internal data flows, such as sharing employee or customer data with subsidiaries outside the EU, such as with offices in the United States or India. This discussion is beyond the scope of this Paper.

[12] *See generally* Landy Kindle, *Everything You Need to Know about Cybersecurity as a Service (CSaaS)*, TECHHEADS, https://blog.techheads.com/everything-you-need-to-know-about-cybersecurity-as-a-service-csaas [https://perma.cc/32B5-ZXYG] (last visited June 17, 2024); *Cybersecurity as a Service*, CLOUDBLUE,

known for its expertise as a Managed Security Service Provider ("MSSP").[13] Based on the contractual relationship between the two companies, TechGuard entrusts ACME Cyber Sentinel to carry out its general cybersecurity objectives by analyzing data sourced from its infrastructure, which spans endpoints, cloud servers, on-premises systems, and employees' mobile devices.[14]

ACME Cyber Sentinel delivers a range of cybersecurity services, including:

- ***Endpoint detection and response:*** This category of services encompasses threat detection and prevention,[15] network intrusion detection,[16] malware detection,[17] and phishing detection.[18]

---

https://www.cloudblue.com/glossary/cybersecurity-as-a-service-csaas/ [https://perma.cc/E26V-ESQR] (last visited June 19, 2024); *What is Cybersecurity-as-a-Service (CSaaS) and How it Can Help Your Business?*, HEIMDAL (Mar. 26, 2024), https://heimdalsecurity.com/blog/cybersecurity-as-a-service-csaas/ [https://perma.cc/JF3F-CTHY].

[13] *See generally* Matthew Finio & Amanda Downie, *What is a Managed Security Service Provider?*, IBM (June 5, 2024), https://www.ibm.com/topics/managed-security-service-provider [https://perma.cc/Q3VD-FM9V]; John Morris et al., *Cyber Security as a Service*, ARXIV (Feb. 22, 2024), https://arxiv.org/pdf/2402.13965v1 [https://perma.cc/6AU8-U75F].

[14] We acknowledge that the provision of state-of-the-art cybersecurity services typically involves the use of machine learning and/or AI tools. For purposes of undertaking step-by-step legal analysis, Scenario 1 discusses ACME Cyber Sentinel providing these cybersecurity services without the mention of AI tools. In Scenario 4, we will return to this topic and explore the analysis noting that ACME Cyber Sentinel is utilizing AI tools.

[15] *What is Threat Detection and Response?*, MICROSOFT, https://www.microsoft.com/en-us/security/business/security-101/what-is-threat-detection-response-tdr [https://perma.cc/R8MH-GNV7] (last visited June 19, 2024); Bart Lenaerts-Bergsmans, *What is Threat Detection, Investigation, and Response (TDIR)?*, CROWDSTRIKE (Feb. 12, 2024), https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/threat-detection-investigation-response-tdir/ [https://perma.cc/TE6E-2QN2]; *What is an ML-Powered NGFW?*, PALO ALTO NETWORKS, https://www.paloaltonetworks.com/cyberpedia/what-is-an-ml-powered-ngfw [https://perma.cc/NSU6-VJ9H] (last visited June 19, 2024).

[16] *What is an ML-Powered NGFW?*, *supra* note 15.

[17] *See Cortex*, PALO ALTO NETWORKS, https://www.paloaltonetworks.com/cortex/cortex-xdr [https://perma.cc/E32T-CTDN] (last visited June 19, 2024).

[18] Ayuns Luz & Edwin Frank, *Data Preprocessing and Feature Extraction For Phishing URL Detection*, RESEARCHGATE (Mar. 10, 2024), https://www.researchgate.net/publication/378804421_Data_preprocessing_and_feature_extraction_for_phishing_URL_detection [https://perma.cc/7TN3-4ZEP]; *see* Dinil Mon Divakaran & Adam Oest, *Phishing Detection Leveraging Machine Learning and Deep Learning: A Review*, IEEE SECURITY & PRIVACY (May 16, 2022), https://arxiv.org/abs/2205.07411 [https://perma.cc/P5LH-7UFD]; *Automated Phishing Incident Response*, IRONSCALES, https://ironscales.com/solutions/secops/ai-powered-phishing-incidence-response/ [https://perma.cc/3GRT-XEEU] (last visited June 19, 2024).

- ***Alert management:*** This category is comprised of alert filtering, alert prioritization, and alert fusion.[19]
- ***Vulnerability management***: This category includes security information and event management ("SIEM"),[20] penetration testing,[21] and threat intelligence.[22]
- ***Identity access management***: This category includes multifactor authentication and privileged access management.[23]

In providing these cybersecurity services, ACME Cyber Sentinel handles numerous types of security telemetry—such as network traffic logs, endpoint activity logs, cloud workloads,[24] and network traffic—gathered from *within*

---

[19] *See Why is Alert Management Essential?*, SECURITI, https://securiti.ai/glossary/alert-management/ (last visited June 19, 2024); Amy Brennen, *Intelligent Alerts and Alert Management Best Practices*, BIGPANDA (Nov. 15, 2023), https://www.bigpanda.io/blog/intelligent-alerts-itops-best-practices/ [https://perma.ccD9KH-CYTH]; Sarah Salis, *Alter Management In Cybersecurity: How to Optimize False Positives*, HARFANGLAB (Mar. 5, 2024), https://harfanglab.io/en/blog/methodology/alert-management-cybersecurity-false-positives/ [https://perma.cc/X98V-A5EB].

[20] *What is SIEM?*, IBM, https://www.ibm.com/topics/siem [https://perma.cc/AH8P-XP2E] (last visited June 19, 2024); *What Is SIEM? - Security Information and Event Management*, CISCO, https://www.cisco.com/c/en/us/products/security/what-is-siem.html [https://perma.cc/MDJ4-XCJ6] (last visited June 19, 2024); *What is SIEM (Security Information and Event Management)?*, CLOUDFLARE, https://www.cloudflare.com/learning/security/what-is-siem/ [https://perma.cc/NNK9-93A7] (last visited June 19, 2024).

[21] *Navigating the Threat Landscape: Understanding Exposure Management, Pentesting, Red Teaming and RBVM*, THE HACKER NEWS (Apr. 29, 2024), https://thehackernews.com/2024/04/navigating-threat-landscape.html [https://perma.cc/L8DU-DNXE]; Michel Ganado & Kirsten Cremona, *Red Teaming and Penetration Testing: What's The Difference?*, PWC MALTA, https://www.pwc.com/mt/en/publications/technology/red-teaming-and-penetration-testing.html [https://perma.cc/V3UZ-QELY] (last visited June 19, 2024).

[22] *What is Vulnerability Management?*, MICROSOFT, https://www.microsoft.com/en-us/security/business/security-101/what-is-vulnerability-management [https://perma.cc/D8LZ-8YX8] (last visited June 19, 2024); Greg Halpin, *Notes from the Field: Center for Internet Security Control 7 – Continuous Vulnerability Management*, KIRKPATRICK PRICE (July 6, 2023), https://kirkpatrickprice.com/blog/notes-from-the-field-center-for-internet-security-control-7-continuous-vulnerability-management/ [https://perma.cc/474N-7TME].

[23] Narendran Vaideeswaran, *Identity Access Management (IAM)*, CROWDSTRIKE (Nov. 17, 2023), https://www.crowdstrike.com/cybersecurity-101/identity-access-management-iam/ [https://perma.cc/WM68-BG2P]; David Strom, *What is IAM? Identity and Access Management Explained*, CSO ONLINE (May 7, 2024), https://www.csoonline.com/article/518296/what-is-iam-identity-and-access-management-explained.html [https://perma.cc/BG9R-45JX].

[24] Telemetry in this setting is "data collected from a network environment that can be analyzed to monitor the health and performance, availability, and security of the network and its components, allowing network administrators to respond quickly and resolve network issues in real-time." *Telemetry for Cybersecurity*, BLACKBERRY,

TechGuard's technology stack that may include personal data such as usernames, internet protocol addresses ("IP addresses"), file names and paths to subject TechGuard's endpoint environment, configurations and naming conventions.[25]

B. Scenario 2 – ACME Cyber Sentinel stores and analyzes limited amounts of information from ten clients on potential cybersecurity threats

ACME Cyber Sentinel contracts with ten businesses ("Businesses 1 to 10") to deliver the cybersecurity services described in Scenario 1. In its operations, ACME Cyber Sentinel stores and analyzes limited amounts of information, considered potential new cyber threats, gathered from each client. The data collected from Businesses 1 to 10 is then consolidated with other datasets held by ACME Cyber Sentinel. Subsequently, ACME Cyber Sentinel may share relevant threat insights with security bulletin publishers that are accessible to other cybersecurity firms.[26] Additionally, ACME Cyber Sentinel may opt to transmit data to an Information Sharing and Analysis Center ("ISAC") for wider dissemination among relevant stakeholders.[27]

---

https://www.blackberry.com/us/en/solutions/endpoint-security/extended-detection-and-response/telemetry [https://perma.cc/8QWS-PTHM] (last visited June 19, 2024); *see* Giovanni Apruzzese et al., *The Role of Machine Learning in Cybersecurity*, DIGITAL THREATS: RESEARCH AND PRACTICE (Mar. 2023), https://dl.acm.org/doi/pdf/10.1145/3545574 [https://perma.cc/S4VF-NUD]; Iqbal Sarker et al., *Cybersecurity Data Science: An Overview from Machine Learning Perspective*, J. BIG DATA 1, 2 (2020); Brandon W. Jackson, *Cybersecurity, Privacy, and Artificial Intelligence: An Examination of Legal Issues Surrounding the European Union General Data Protection Regulation and Autonomous Network Defense*, 21 MINN. J.L. SCI. & TECH. 169, 184 (2020); Anshu Bansal, *What is Cloud Workload? Types, Challenges & Best Practices*, CLOUDDEFENSE.AI (Mar. 18, 2024), https://www.clouddefense.ai/what-is-cloud-workload/ [https://perma.cc/42LU-24UY].

[25] Alexander S. Gillis, *What Is Network Traffic?*, TECHTARGET (Dec. 2022), https://www.techtarget.com/searchnetworking/definition/network-traffic [https://perma.cc/TLL4-RPG5]; *What is Network Traffic?*, FORTINET, https://www.fortinet.com/resources/cyberglossary/network-traffic [https://perma.cc/3JYA-Z36X] (last visited June 19, 2024); *see* Soundarya Jayaraman, *Network Traffic Analysis (NTA): What It Is and Why It Matters*, G2.COM (July 17, 2023), https://www.g2.com/articles/network-traffic-analysis [https://perma.cc/7SPQ-SDEZ]. For phishing detection, ACME Cyber Sentinel undertakes content analysis of emails, including inspection of the URLs within emails. *See* Luz & Frank, *supra* note 18; *Automated Phishing Incident Response*, *supra* note 18; Divakaran & Oest, *supra* note 18.

[26] *See Overview About the CVE Program*, CVE, https://www.cve.org/About/Overview [https://perma.cc/G5YJ-XB5R] (last visited June 19, 2024); *History*, CVE, https://www.cve.org/About/History [https://perma.cc/BX2N-KGPM] (last visited June 19, 2024); *National Vulnerability Database*, NIST (May 29, 2024), https://nvd.nist.gov/ [https://perma.cc/28FC-UG6F].

[27] *What is an ISAC?*, CTR. INTERNET SECURITY, https://www.cisecurity.org/isac [https://perma.cc/AT9R-RTLB] (last visited June 19, 2024); *Information Sharing and*

C. Scenario 3 – ACME Cyber Sentinel uses data collected from ten clients for training, evaluating, and deploying AI cybersecurity tools

ACME Cyber Sentinel leverages data collected from Businesses 1 to 10 for the training, evaluation, and deployment of advanced ML algorithms utilized in AI cybersecurity tools where ML algorithms are integral to its state-of-the-art cybersecurity services.[28] Cybersecurity companies use these algorithms for threat detection and prevention, alert management, vulnerability management, and identity and access management.[29]

The ML training process entails data collection and preparation, feature engineering, and model training. ACME Cyber Sentinel ***collects*** relevant cybersecurity data from each of the ten client businesses for training the model by contextualizing, correlating, and processing complex and nuanced data records. More data improves the ability to spot signals.[30] For most cybersecurity tools, this data comprises security telemetry, such as network traffic logs, endpoint activity logs, threat intelligence feeds, and other cyber threat information. It is worth noting that behavioral analytics, which involve training algorithms to understand normal entity behavior and user behavior within a system, can be particularly useful for detection and prevention, vulnerability management, and identity management.

Behavioral analytics, for example, can help identify when an account is accessed from an unusual browser, device, or geographic location.[31] Also, behavioral analytics can help confirm the identity of a customer or an employee using techniques such as keystroke analysis.[32] This type of

---

Analysis Centers (ISACs), ENISA, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing [https://perma.cc/2N9M-4FNC] (last visited June 19, 2024).

[28] *See* Apruzzese et al., *supra* note 24, at 1; Frank Schweitzer et al., *The Rise of Artificial Intelligence, Big Data, and the Next Generation of International Rules Governing Cross-Border Data Flows and Digital Trade*, WHITE & CASE LLP (Mar. 14, 2024), https://www.whitecase.com/insight-our-thinking/rise-artificial-intelligence-big-data-next-generation-international-rules [https://perma.cc/258B-XR2P].

[29] *See generally* Apruzzese et al., *supra* note 24.

[30] *See* Sven Krasser, *How Human Intelligence Is Supercharging CrowdStrike's Artificial Intelligence*, CROWDSTRIKE (Apr. 8, 2022), https://www.crowdstrike.com/blog/how-human-intelligence-is-supercharging-crowdstrike-artificial-intelligence/ [https://perma.cc/357Z-8LVS].

[31] The term "behavioral analytics" refers to "studying the tendencies and activity patterns of an organization's users." Lucia Stanham, *Behavioral Analytics*, CROWDSTRIKE (November 14, 2023), https://www.crowdstrike.com/cybersecurity-101/secops/behavioral-analytics/ [https://perma.cc/2Z6M-SZU4].

[32] Lulu Yang et al., *TKCA: A Timely Keystroke-Based Continuous User Authentication With Short Keystroke Sequence In Uncontrolled Settings*, 4 CYBERSECURITY 1 (2021); Ben Canner, *What are Keystroke Dynamics? How Can It Improve Your Authentication?*, SOLUTIONS REV. (June 25, 2020), https://solutionsreview.com/identity-management/what-are-keystroke-dynamics-how-can-it-improve-your-authentication/ [https://perma.cc/4GD8-72M8]; Soumen Roy et al., *A Systematic*

information can assist in detecting advanced persistent threats ("APTs"), detecting insider threats, and identifying potential new threats.[33] To establish the expected behaviors of users, these behavioral analytics tools may collect both personal data and sensitive personal data, such as the typical locations of users or of their devices as well as patterns in keystrokes that can indicate certain medical conditions.[34] Assume for purposes of this scenario that the company does not use the information collected for cybersecurity behavioral analytics for any behavioral advertising or other marketing to individuals whose data is processed for cybersecurity purposes.

Before training the ML algorithms, ACME Cyber Sentinel ***prepares the data*****,** referred to as pre-processing, which entails "cleaning" the collected data to ensure consistency and accuracy. Data cleaning refers to removing duplicates, handling missing values, and standardizing data formats.[35] A poorly trained model with unprepared data may produce incorrect predictions, generate a flurry of false positives, and, as a result, undermine protection efficiency.[36]

Once ACME Cyber Sentinel prepares the data, it ***engineers meaningful features*** (e.g., an abnormal login time pattern for user accounts within a client's network) from the collected data. These features serve as inputs to the ML algorithms and capture essential information about cybersecurity threats like network traffic patterns. Finally, ACME Cyber Sentinel ***trains its ML models*** to detect and mitigate various cyber threats, including malware, phishing attacks, and unauthorized access attempts. The training process involves feeding labeled data that indicates, for example, whether an event is

---

Literature Review on Latest Keystroke Dynamics Based Models, 10 IEEE ACCESS 92192 (2022).

[33] Bart Lenaerts-Bergmans, *Advanced Persistent Threat (APT)*, CROWDSTRIKE (Feb. 28, 2023), https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/ [https://perma.cc/J938-ASDY] ("An advanced persistent threat (APT) is a sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network in order to steal sensitive data over a prolonged period of time. An APT attack is carefully planned and designed to infiltrate a specific organization, evade existing security measures and fly under the radar."); *see* George Karantzas & Constantinos Patsakis, *An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors*, 1 J. CYBERSECURITY & PRIV. 387–421 (2021).

[34] Shanika Wickramasinghe, *Behavioral Analytics in Cybersecurity*, SPLUNK BLOGS (Mar. 9, 2023), https://www.splunk.com/en_us/blog/learn/behavioral-analytics.html [https://perma.cc/JVS8-8DGJ]; Lucia Stanham, *Behavioral Analytics*, CROWDSTRIKE (Nov. 14, 2023), https://www.crowdstrike.com/cybersecurity-101/secops/behavioral-analytics/ [https://perma.cc/MCY9-ELAP]; Lucia Stanham, *What is AI-Powered Behavioral Analysis In Cybersecurity*, CROWDSTRIKE, (Sept. 7, 2023), https://www.crowdstrike.com/cybersecurity-101/secops/ai-powered-behavioral-analysis/ [https://perma.cc/4MM5-NP88].

[35] *ML - Overview of Data Cleaning*, GEEKSFORGEEKS (May 24, 2024), https://www.geeksforgeeks.org/data-cleansing-introduction/ [https://perma.cc/SDV2-VUGH].

[36] *See* Krasser, *Why Machine Learning Is a Critical Defense Against Malware*, *supra* note 8.

benign or malicious, into the models and adjusting their parameters to optimize performance.[37]

Before ACME Cyber Sentinel can deploy its ML model, it must evaluate the performance of its ML models using separate validation datasets that belong to Businesses 1 to 10. During the model training process, ACME Cyber Sentinel sets aside a portion of the data collected from Businesses 1 to 10 for validation. This validation dataset is representative of the broader dataset used to train the ML models but should not be directly used in the training process to ensure unbiased evaluation. By using data from the same training dataset for validation, ACME Cyber Sentinel can assess how well the training ML models generalize unseen data from the same sources using real-world scenarios. Once validated, ACME Cyber Sentinel deploys the trained ML models into its cybersecurity infrastructure, continuously analyzing incoming data streams from client networks and endpoints in real time. These models enhance ACME Cyber Sentinel's ability to detect and respond to cyber threats quickly, mitigating the risk of future breaches and data loss for Businesses 1 to 10.

D. Scenario 4 – ACME Cyber Sentinel utilizes these state-of-the-art AI cybersecurity tools when it provides cybersecurity services to TechGuard

Scenario 1 detailed how ACME Cyber Sentinel provides its cybersecurity services to TechGuard. In Scenario 4, ACME Cyber Sentinel utilizes state-of-the-art AI cybersecurity tools to do so.[38] While ACME Cyber Sentinel oversees the management of these tools, much of the data collection for cyber defense and remediation is automated through these tools.[39]

As with Scenario 3, much of the data that the deployed AI cybersecurity tools use will be security telemetry. When utilizing behavioral analytics trained on expected entity and user behavior within a system, these tools will compare the typical behaviors with incoming information to identify

---

[37] Sumit Singh, *Everything You Need to Know About AI Model Training*, LABELLERR (Apr. 30, 2023), https://www.labellerr.com/blog/everything-you-need-to-know-about-ai-model-training/ [https://perma.cc/G6A9-2ZCB]; *Model Training in AI/ML: Process, Challenges, and Best Practices*, KOLENA (Apr. 18, 2024), https://www.kolena.com/guides/model-training-in-ai-ml-process-challenges-and-best-practices/ [https://perma.cc/NPB5-672J].

[38] This is sometimes referred to in the industry as a "threat feed provider," but much of these algorithms are disseminated via regular updates into the cyber security tools mentioned in Scenario 2. *See* Bart Lenaerts-Bergmans, *What is a Threat Intelligence Feed?*, CROWDSTRIKE (May 5, 2023), https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/threat-intelligence-feeds/ [https://perma.cc/J2V5-92FJ].

[39] Apruzzese et al., *supra* note 24, at 4; *see* Sarker et al., *supra* note 24, at 3; Jackson, *supra* note 24, at 201.

anomalous behavior as potential threats.[40] When used by ACME Cyber Sentinel, these tools may collect personal data or sensitive personal data from TechGuard, such as current locations of users or their devices or the keystrokes of customers or employees (which could, for instance, indicate sensitive data such as medical conditions).

III. OVERVIEW OF RELEVANT LEGAL REQUIREMENTS IN THE EU

This Part provides a primer related to the legal requirements of the GDPR. In addition, it includes an introduction to the newly passed AI Act.

A. EU's GDPR

Understanding the obligations in the GDPR is critical to determining the types of legal responsibilities ACME Cyber Sentinel has in relation to the cybersecurity services it provides to TechGuard. The GDPR is an EU regulation focused on data privacy. Companies doing business in the EU, like ACME Cyber Sentinel, are legally obligated to comply with the comprehensive privacy requirements set forth in the GDPR.[41] The definition found in the GDPR for "personal data," as well as the distinctions between "controller" and "processor," provide initial guidance as to what types of data the regulation covers and the level of responsibility that ACME Cyber Sentinel will have for such covered data. Key legal responsibilities in the GDPR include: requirements for processing data, fulfillment of obligations related to individual rights, and rules for international transfers.[42]

---

[40] Wickramasinghe, *supra* note 34; Stanham, *Behavioral Analytics*, *supra* note 34; Stanham, *What is AI-Powered Behavioral Analysis In Cybersecurity*, *supra* note 34.

[41] "The GDPR introduces two principles with regard to territorial applicability: establishment and extra-territorial effect." Matthias Artzt, *Territorial Scope of the GDPR from a U.S. Perspective*, IAPP (June 26, 2018), https://iapp.org/news/a/territorial-scope-of-the-gdpr-from-a-us-perspective/ [https://perma.cc/WEP9-LH2D]. In other words, the GDPR applies to companies that are established in the EU as well as to companies that are not established in the EU, if those companies handle EU data in certain prescribed ways. *Id.*

[42] GDPR, *supra* note 1; *see* EUR. COMM'N, DATA PROTECTION (2022); *see* Jan Dhont et al., *The EU General Data Protection Regulation – Europe Adopts Single Set of Privacy Rules*, ALSTON & BIRD PRIVACY & DATA SECURITY BLOG (Dec. 16, 2015), www.alstonprivacy.com/the-eu-general-data-protection-regulation-europe-adopts-single-set-of-privacy-rules/ [https://perma.cc/G5H9-5EPJ].

1. Personal Data

The GDPR broadly defines personal data as "any information relating to an identified or identifiable natural person."[43] If data can be grouped together to lead to an identification, the pieces generally constitute personal data.[44]

Categories of potential personal data relevant to cybersecurity include:

1. Data that explicitly mentions a natural person (e.g., a database of users).

2. Data that is derived from the activity of a natural person (e.g., log files which relate to a user's activity, or which contain references to users).

3. Data that contains information which could be used to identify a natural person, given some other information that is not held by the controller.[45]

Notably, the European courts have broadly interpreted the term "personal data" as defined by the GDPR.[46] Under EU law, artifacts such as IP addresses do not contain any personal data in and of themselves, nor do they automatically grant the processor access to personal data. IP addresses in fact come within the definition of personal data if there exists a legal right for the processor to compel the release of the personal data under any circumstance.[47] In *Patrick Breyer v. Bundesrepublik Deutschland*, the Court

---

[43] GDPR, *supra* note 1, art. 4(1); *see* EUR. COMM'N, WHAT IS PERSONAL DATA?, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en [https://perma.cc/28YV-5SS4] (last visited June 19, 2024); *see generally* Leon Böck et al., *Processing of Botnet Tracking Data under the GDPR*, 5 COMPUT. L. & SEC. REV. 3 (2022).

[44] Patrick Breyer v. Bundesrepublik Deutschland, Case C-582/14, ¶ 14, Bundesgerichtshof [BGH] [Federal Court of Justice] Oct. 19, 2016.

[45] *See* Böck et al., *supra* note 43, at 5.

[46] Two cases which examine this issue in detail are *Breyer* and *Nowak*. *Patrick Breyer*, Case C-582/14; Nowak v. Data Protection Comm'r, Case C-434/16 Supreme Court (Ireland), Dec. 20, 2017. Although both of these cases were examined under the 1995 Data Protection Directive, as opposed to the GDPR, the Court of Justice of the European Union (the "CJEU"), the senior court constituted within the European Union, has held that the interpretations of personal data remain valid under the GDPR. Directive 95/46/EC On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data, O.J. (L 281), 23/11/1995 P. 0031-0050 (1995); COURT OF JUSTICE OF THE EUROPEAN UNION, GENERAL PRESENTATION, https://curia.europa.eu/jcms/jcms/Jo2_6999/ [https://perma.cc/35XU-R5BD] (last visited June 19, 2024); see also Single Resolution Board (SRB) v. European Data Protection Supervisor (EDPS), Case T-557/20, ¶ 60, Apr. 26, 2023, for affirmation of the *Nowak* judgment under the GDPR and *id.* ¶ 88 for a similar affirmation of the *Breyer* judgment.

[47] *Patrick Breyer*, C-582/14 ¶ 47.

of Justice for the European Union ("CJEU") examined whether an IP address, when processed by an entity other than an internet service provider ("ISP"), could also constitute personal data.[48] Focusing on the inclusion of the term "indirectly" in the definition of personal data,[49] the CJEU concluded that where there is the legal potential for the processor of the IP address to obtain the data subject's identity, then the IP address constitutes personal data.[50] The mere existence, under German law, of the mechanism to seek Breyer's identity following a cyberattack (despite an absence of any suggestion that Breyer was a cyberattacker) was sufficient to ensure that dynamic IP addresses are deemed personal data—at least in Germany (or any other EU member state) where there is a legal mechanism to compel an ISP to release the identity of the registered user of the IP address. *Nowak v. Data Protection Commissioner* affirmed this broad view of the definition of personal data, where the CJEU examined both the content of the data and the context in which the data was used in relation to the individual.[51]

The GDPR also identifies "special categories of personal data" that receive additional protections under the GDPR.[52] These sensitive categories of personal data are defined as "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data [to] uniquely identify[] a natural person, data concerning health or data concerning a natural person's sex life

---

[48] *Id.* ¶ 14. The court noted how there are two forms of IP address: a "static" IP address which does not change over time, and a dynamic IP address, which changes each time the user accesses the internet. *Id.* ¶ 16. Mr. Breyer was using a dynamic IP address. *Id.* ¶ 20. The court relied on an earlier judgment in *Scarlet Extended*, which affirmed that IP addresses constitute personal data when processed by an Internet Service Provider (an "ISP"). Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), Case C-70/10 51 (2011).

[49] *Patrick Breyer*, C-582/14 ¶ 14. This term is also included in the GDPR's definition of personal data. GDPR, *supra* note 1, art. 4(1).

[50] *Patrick Breyer*, C-582/14 ¶ 49.

[51] *Nowak*, C-434/16 at 31; *Patrick Breyer*, C-582/14 ¶ 33. The facts of *Nowak* differ from those of *Breyer*, as the claimant was a trainee accountant who sought access to his exam scripts which were held by the Institute of Chartered Accountants of Ireland (the "CAI"). *Nowak*, C-434/16 ¶¶ 18–26. CAI alleged that the exam script was not personal data. *Id.* ¶¶ 20–21. However, the court held that the examination ID number allowed each script to be identified by the CAI and so constituted personal data, and the nature of the exam itself is a means to establish an individual's performance and not to obtain data that is independent of the individual themselves, and so must be considered as personal data. *Id.* ¶¶ 29, 41, 61.

[52] *GDPR*, *supra* note 1, art. 9; *see* EUR. COMM'N, WHAT PERSONAL DATA IS CONSIDERED SENSITIVE? (2022); *see also* Natasha Lomas, *Sensitive Data Ruling by Europe's Top Court Could Force Broad Privacy Reboot*, TECHCRUNCH (Aug. 2, 2022, 12:55 PM), https://techcrunch-com.cdn.ampproject.org/c/s/techcrunch.com/2022/08/02/cjeu-sensitive-data-case/amp/ [https://perma.cc/PNU6-FWDW]; *see generally* Amber Boehm, *General Data Protection Regulation (GDPR)*, CROWDSTRIKE (June 16, 2023), https://www.crowdstrike.com/cybersecurity-101/data-security/general-data-protection-regulation-gdpr/ [https://perma.cc/EJ87-JTFN].

or sexual orientation."[53] For processing special categories of personal data, the additional obligation most applicable to cybersecurity companies is the requirement for explicit consent from the data subject as the lawful basis for processing rather than legitimate interests or the performance of a contract, which are not permitted.[54] For explicit consent, the individual must typically "give an express statement of consent."[55] While processing special categories of data is not generally the focus of cybersecurity services, such data may be included in the overall data used for the services.

2. Controller and Processor

Understanding the distinction between controller and processor is important in determining a company's legal responsibilities under the GDPR. A data "controller" is a natural or legal person who determines the purposes and means of processing personal data.[56] In a particular processing activity, the controller is the entity that determines "*why* the processing is taking place (i.e., 'to what end'; or 'what for?') and *how* this objective shall be reached (i.e., which means shall be employed to obtain the objective)."[57] The controller is responsible for ensuring the rights of the data subject and

---

[53] GDPR, *supra* note 1, art. 9(1). In the United States, geolocation data is often considered a sensitive category of personal data. Jason Sarfati, *Making the Case for a New Geolocation Data Privacy Paradigm*, IAPP (Aug. 25, 2022), https://iapp.org/news/a/making-the-case-for-a-new-geolocation-data-privacy-paradigm/ [https://perma.cc/YR2A-V4A2]. Under the GDPR, geolocation data is considered personal data but does not currently fall into a special category of data. *See* Cobun Zweifel-Keegan, *A View from DC: Updating the Map of Location Privacy Safeguards*, IAPP (Jan. 24, 2024), https://iapp.org/news/a/a-view-from-dc-updating-the-map-of-location-privacy-safeguards [https://perma.cc/6KEF-3TEL] ("The EU General Data Protection Regulation famously omits precise geolocation data from the list of special categories of personal data."); Sarfati, *supra* note 53.

[54] GDPR, *supra* note 1, art. 9(2).

[55] *Guidelines 05/2020 on Consent Under Regulation 2016/679*, 93 (May 4, 2020), EDPB, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf [https://perma.cc/44UY-W28L] [hereinafter *Guidelines on Consent*]. "A data controller may . . . obtain explicit consent from a visitor to its website by offering an explicit consent screen that contains Yes and No check boxes, provided that the text clearly indicates the consent, for instance 'I, hereby, consent to the processing of my data,' and not for instance, 'It is clear to me that my data will be processed.'" *Id.* ¶ 96.

[56] GDPR, *supra* note 1, art. 4(7). In layman's terms, a natural person is an individual while a legal person can be thought of as a business.

[57] EDPB, *Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR* (version 2.1), ¶ 35 (July 7, 2021), https://www.edpb.europa.edu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf [https://perma.cc/P9M8-KSJ3] [hereinafter *Guidelines on the Concepts of Controller and Processor*] (emphasis in original). The EDPB states, "Dictionaries define 'purpose' as 'an anticipated outcome that is intended or that guides your planned actions' and 'means' as 'how a result is obtained or an end is achieved.'" *Id.* ¶ 33.

ensuring (and demonstrating) that the processing of all personal data is in accordance with the GDPR requirements.[58] This means that the controller must ensure that the personal data: is processed in a lawful, fair, and transparent manner;[59] is for specified, explicit, and legitimate purposes;[60] is limited to what is necessary for the processing purpose;[61] is accurate and only allows the data subject to be identified for no longer than is necessary to achieve the objective of the processing;[62] is kept up to date (if necessary);[63] and is processed in a secure manner.[64] Therefore, the data controller is obligated to collect only personal data that is directly relevant to their processing objectives and is required to keep this personal data only as long as necessary.

A data "processor" is a legal or natural person who processes personal data on behalf of and in a manner determined by the controller.[65] The processing activity of the processor can be thought of as an "ancillary task that is carried out as part of the client company's activity."[66] The GDPR requires the processor to be governed by instructions provided by the controller in a contract.[67] Where a processor engages in the processing of personal data that goes beyond the scope of the activity authorized by the controller, the processor shall be considered a controller with regard to this activity.[68] There is a positive burden on processors to ensure that their processing activities, which the controller sets out, are lawful and in compliance with the GDPR. Notably, processors can be found liable for damages arising from unlawful

---

[58] GDPR *supra* note 1, art. 24.

[59] *Id.* art. 5(1)(a).

[60] *Id.* art. 5(1)(b).

[61] *Id.* art. 5(1)(c).

[62] *Id.* art. 5(1)(e).

[63] *Id.* art. 5(1)(d).

[64] *Id.* art. 5(1)(f).

[65] *Id.* art. 4(8). Although not mentioned in the legislation, it is common to find references to 'sub-processors' who are processors which process data on-behalf of a data-processor although the consent of the controller is required for such an operation. *Id.* at 29.

[66] *Guidelines on the Concepts of Controller and Processor*, *supra* note 57, ¶ 40 (outlining Accountants as an example).

[67] GDPR, *supra* note 1, art. 4(20); *id.* art. 28(2); *see* Kumar Venkatesh & Teodora Pimpireva, *The Processor: Always a Bridesmaid, Never a Bride, Privacy Tracker*, IAPP (Oct. 30, 2018), https://iapp.org/news/a/the-processor-awakens-episode-gdpr/ [https://perma.cc/9DNZ-769G]. For a detailed discussion of processors obligations, see Detlev Gabel and Tim Hickman, *Chapter 11: Obligations of Processors – Unlocking the EU General Data Protection Regulation*, WHITE & CASE LLP (Apr. 5, 2019), https://www.whitecase.com/publications/article/chapter-11-obligations-processors-unlocking-eu-general-data-protection [https://perma.cc/4P7H-HFQ4].

[68] GDPR, *supra* note 1, art. 28(10).

processing, even when the processor has complied with the controller's instructions but failed to comply with the GDPR.[69]

In its guidelines on the concepts of controller and processor in the GDPR, the European Data Protection Board ("EDPB") explains that the distinction between a processor and a controller is a fact-specific inquiry—with the classic "it depends" on the details of the situation.[70] When an entity provides detailed instructions on processing, is instructed how long to retain data, and does not process the data for its own purposes, then the entity is likely a processor under the GDPR.[71] Notably, an entity may simultaneously act as a processor for certain processing activities and as a controller for other processing activities.[72]

Although the determination of whether ACME Cyber Sentinel is acting as a processor or controller is based on an assessment of factual circumstances, a contract between ACME Cyber Sentinel and its client(s) can be helpful to document the expectations of the parties, to explain who is involved in determining the types of processing activities that will take place and the purposes of such processing, and to provide detailed instructions for processing (when appropriate).[73] Even though the contract does *not* determine the status of a party as a processor or controller under EU law, a contract can facilitate the determination of the role of each party, particularly to the extent that the contract reflects the actual relationship between the parties.[74]

Importantly, the legal framework created by the GDPR allows for more than one controller of the data in a particular transaction involving personal data—referred to as joint controllers.[75] For joint controllership to exist, there

---

[69] *I*d. art. 82(2).

[70] "The question is where to draw the line between decisions that are reserved to the controller and decisions that can be left to the discretion of the processor. Decisions on the purpose of the processing are clearly always for the controller to make." *Guidelines on the Concepts of Controller and Processor*, *supra* note 57, ¶ 39.

[71] *Id.* ¶¶ 15–84; *see id.* at 49–51.

[72] The EDPB points out that "the same entity may act at the same time as a controller for certain processing operations and as a processor for others, and the qualification as controller or processor has to be assessed with regard to specific sets of data or operations." *Id.* ¶ 82.

[73] "In many cases, an assessment of the contractual terms between the different parties involved can facilitate the determination of which party (or parties) is acting as controller." *Id.* ¶ 28.

[74] "However, . . . [i]t is not possible either to become a controller or to escape controller obligations simply by shaping the contract in a certain way where the factual circumstances say something else." *Id.* "If one party in fact decides why and how personal data are processed that party will be a controller even if a contract says that it is a processor." *Id.* ¶ 29; *see id.* ¶¶ 28–30; *see id.* ¶ 81 (providing an example of a service provider referred to as data processor but acting as controller).

[75] Article 26 of the GDPR details the definition of "joint controllers." GDPR, *supra* note 1, art. 26. This concept has certain similarities to a "joint venture" in United States law. *See* Marshall Hargrave, *Joint Venture (JV): What It Is, and Why Do Companies Form One?*, INVESTOPEDIA (June 14, 2024), https://www.investopedia.com/terms/j/jointventure.asp [https://perma.cc/A6SZ-7EP9] ("A joint venture (JV) is

must be joint participation by the entities in determining the means and purposes for the processing activity—meaning that each entity must exercise influence over the how and why of the processing.[76] This joint participation can take place through a common decision or converging decisions. Article 26 of the GDPR talks of joint participation in terms of the entities "jointly" making a decision based on a common intention—a common decision.[77] Case law of the CJEU provides the details of converging decisions, where the decisions of two (or more) parties "converge" so that each party's processing is "inextricably linked" to the extent that the processing could not be accomplished without both parties' participation in the purposes and means.[78] With regard to the purposes and means (but not as to other aspects of the relationship between the two parties), joint participation through converging decisions can be said to exist where: (1) the decisions "complement each other"; and (2) the decisions are "necessary for the processing to take place in such manner that they have a tangible impact on the determination of the purposes and means of the processing."[79]

3. Processing Personal Data

For the EU, the GDPR covers a company's processing of personal data.[80] The term "processing" is straight-forward and broad; it encompasses "any

---

a business arrangement in which two or more parties agree to pool their resources for the purpose of accomplishing a specific task. This task can be a new project or any other business activity. Each of the participants in a joint venture is responsible for profits, losses, and costs associated with it."); *but see id.* ("However, the venture is its own entity, separate from the participants' other business interests.").

[76] *Guidelines on the Concepts of Controller and Processor*, *supra* note 57, ¶ 53.

[77] "Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers." GDPR, *supra* note 1, art. 26; *see Guidelines on the Concepts of Controller and Processor*, *supra* note 57, ¶ 55.

[78] *Guidelines on the Concepts of Controller and Processor*, *supra* note 57, ¶ 55; *see* Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV, Case C-40/17 [Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany)] July 29, 2019; Tietosuojavaltuutettu v. Jehovan todistajat, Case C-25/17, Korkein hallinto-oikeus [Supreme Administrative Court, Finland] July 10, 2023; Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH, Case C-210/16, Bundesverwaltungsgericht [Federal Administrative Court, Germany] June 5, 2018 (*Facebook Fanpage Case*); Google Spain SL V. Agencia Española de Protección de Datos (AEPD), Case C-131/12 [Request for a Preliminary Ruling from the Audiencia Nacional of Spain] May 13, 2014; *see also* Manuel Klar, *Binding Effects of the European General Data Protection Regulation (GDPR) on U.S. Companies*, 11 HASTINGS SCI. TECH. LAW J. 101, 105, 138 (2020).

[79] *Guidelines on the Concepts of Controller and Processor*, *supra* note 57, ¶ 55; *see id.* ¶¶ 56–58.

[80] Processing of personal data by European Institutions and agencies is not covered under the GDPR, but instead under a distinct "public sector" counterpart of the GDPR. GDPR, *supra* note 1, at 4. Law enforcement processing of data is not

operation or set of operations which [are] performed on personal data or sets of personal data."[81] Regardless of whether ACME Cyber Sentinel is headquartered inside or outside of the EU, these processing requirements will apply.

One of the most important principles of processing personal data under the GDPR is that the processing must be "lawful."[82] Article 6 of the GDPR outlines the processing of ordinary categories of data.[83] Article 9 explicitly prohibits the processing of special categories of data but provides ten bases for lawfully processing special categories of data.[84] If a controller or processor is unable to demonstrate that their processing complied with either Article 6 or Article 9, then that processing of personal data will most likely be deemed unlawful. To avoid sanction by a Data Protection Agency ("DPA") or a civil action by an individual, [85] it is imperative that any company engaged in the processing of personal data, whether they are a processor or controller, ensures that the basis of their processing meets the lawfulness requirements under the GDPR.

---

covered by the GDPR. Directive 2016/680 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, And Repealing Council Framework Decision 2008/977/JHA, 2016 O.J. (L 119) 1 [hereinafter Directive on the Protection of Natural Persons]. It is important to note that while the GDPR is a regulation, and therefore the text of the regulation is directly applicable and uniform across every Member State, the Law Enforcement directive is a directive, and so the specific text may vary from Member State to Member State. *Id.* However, the text of the Directive will act as a minimum set of data protection requirements for law enforcement activities. *See* Regulation 2018/1725 on the Protection of Natural Persons With Regard to the Processing of Personal Data by the Union Institutions, Bodies, Offices and Agencies and on the Free Movement of Such Data, and Repealing Regulation (EC) No. 45/2001 and Decision No. 1247/2002/EC, 2018 O.J. (L 295) 1.

[81] GDPR, *supra* note 1, art. 4(2).

[82] See *id.* at 6 for the list of requirements associated with the processing of personal data; see *id.* at 9 for the requirements associated with the processing of "special" categories of personal data.

[83] *Id.* art. 6(1).

[84] *Id.* arts. 9(1)–(2). These bases are similar to those listed in Article 6(1), with the exception of "legitimate interests," and include exceptions required for public health and the provision of medical services. *Id.*

[85] *What are Data Protection Authorities (DPAs)?*, EUR. COMM'N, https://commission.europa.eu/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en [https://perma.cc/8DG6-XS6F] (last visited Aug. 23, 2024) ("DPAs are independent public authorities that supervise, through investigative and corrective powers, the application of the data protection law. They provide expert advice on data protection issues and handle complaints lodged against violations of the General Data Protection Regulation and the relevant national laws. There is one in each EU Member State.").

Consent is listed as a lawful basis for processing under the GDPR.[86] Because these scenarios focus on a contractual relationship between two companies—ACME Cyber Sentinel and TechGuard—this Paper discusses the significant limitations of using consent here, partly to explain why this basis is generally not examined in this Paper's scenarios.[87]

The GDPR defines "consent" as "freely given, specific, informed, and an unambiguous indication of the data subject's wishes."[88] In *Planet49*, the CJEU examined whether a pre-ticked checkbox constituted valid consent.[89] The CJEU found that companies must provide their users with enough information to enable them to evaluate the consequences of providing their consent, and then the user must be allowed to undertake a positive action to confirm their consent.[90] Because the pre-ticked checkbox did neither, the company did not obtain valid consent.[91]

The GDPR does not clarify what constitutes a disclosure to inform users of the potential consequences of providing consent, and so far, the CJEU has not provided a specific analysis of this requirement.[92] Accordingly, if

---

[86] GDPR, *supra* note 1, art. 6(1)(a); *see id.* art. 9(2)(a); Jackson, *supra* note 24, at 191; Matthew Humerick, *Taking AI Personally: How the EU Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence*, 34 SANTA CLARA HIGH TECH. L.J. 393, 405 (2018).

[87] *See* Böck et al., *supra* note 43, at 8. For United States practitioners, the definition of consent in the GDPR may be much more detailed and elaborate than expected.

[88] *See* Detlev Gabel & Tim Hickman, *Chapter 5: Key Definitions – Unlocking the EU General Data Protection Regulation*, WHITE & CASE LLP (Apr. 5, 2019), https://www.whitecase.com/insight-our-thinking/chapter-5-key-definitions-unlocking-eu-general-data-protection-regulation [https://perma.cc/4ES6-EUFP]; *see also* Andrew Clearwater & Brian Philbrook, *Practical Tips for Consent under the GDPR*, IAPP (Jan. 23, 2018), https://iapp.org/news/a/practical-tips-for-consent-under-the-gdpr/ [https://perma.cc/8SAK-U4WJ]; Mark Young & Joseph Jones, *EU Regulators Provide Guidance on Notice and Consent Under GDPR*, 14 NAT'L L. REV. (Dec. 14, 2017), https://www.natlawreview.com/article/eu-regulators-provide-guidance-notice-and-consent-under-gdpr [https://perma.cc/F58S-8DHT].

[89] Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e V., Case C-673/17 [Federal Court of Justice, Germany] Mar. 21, 2019. Although the case was heard under the Privacy Directive, the court made explicit reference to the GDPR in their judgment. *Id.* ¶ 41; *see* Lennart Schüßler, Planet 49: *CJEU Rules on Cookie Consent*, BIRD & BIRD (Oct. 2, 2019), https://www.twobirds.com/en/insights/2019/global/planet49-cjeu-rules-on-cookie-consent [https://perma.cc/JGU2-RH6G].

[90] *Planet49*, Case C-673/17 ¶¶ 65, 74. The information listed in Article 13 of the GDPR also be provided to the user before they grant their consent. *Id.* ¶ 76.

[91] *Id.* ¶ 41.

[92] It has been noted in the literature how the specific requirements associated with the 'transparency' obligations imposed by the GDPR are under-regulated and under-litigated. See, e.g., Alexander J. Wulf & Ognyan Seizov, *"Please Understand We Cannot Provide Further Information": Evaluating Content and Transparency of GDPR-Mandated AI Disclosures*, 39 AI SOC. 235, 237–238 (2024) for a discussion

TechGuard sought to use consent as a lawful means of processing personal data for cybersecurity activities, it may be sufficient for TechGuard to seek consent in the relevant privacy policy, informing users that the personal data generated from their interactions with TechGuard's systems will be transferred to ACME Cyber Sentinel to ensure TechGuard's cybersecurity. TechGuard may also want to disclose that this data may be processed in conjunction with other data held by ACME Cyber Sentinel. Without a ruling from the CJEU, it is unclear what disclosures are necessary and what constitutes sufficient disclosure under the GDPR.

The conditions for obtaining valid consent are outlined in Article 7 of the GDPR and only apply when consent is the sole basis for lawful processing.[93] If TechGuard relies on more than one lawful basis, Article 7 will only apply to the processing that relies on the data subject's consent.[94] One of the core elements of consent is that companies cannot obtain it in an unfair contractual bundle.[95] Article 7(4) of the GDPR explores this by examining whether companies tie consent for processing personal data to acceptance of the overarching contract and whether or not the contract as a whole requires consent.[96]

The EDPB has issued clear guidance on the "conditionality" of consent when companies bundle it with other agreements,[97] and it suggests that when bundled with other agreements that do not require the processing of personal data, the data subject's consent will be invalid. Thus, if ACME Cyber Sentinel bundles the use of their services with consent for the processing of the data subject's personal data and is unable to demonstrate why it requires consent for the delivery of its service in its entirety, then a DPA or the CJEU may invalidate the user consent agreement.

Given the specific nature of the TechGuard and ACME Cyber Sentinel relationship, there could be several challenges in using consent to legally process personal data. The first is that if the individual withholds consent, TechGuard will lose the ability to process the individual's information for cybersecurity purposes and will consequentially lose the ability to determine the legitimacy of a subset of their users. Furthermore, it is a condition of valid consent that the data subject can revoke it at any time.[98] Therefore, ACME Cyber Sentinel can only process the data subject's personal data for as long as the data subject has not revoked their consent.

---

about how controllers have obfuscated the specific processing activities in both "traditional" and "algorithmic" processing activities.

[93] GDPR, *supra* note 1, art. 7(1).

[94] *See id.* art. 7(4) ("When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.").

[95] *Guidelines on Consent*, *supra* note 55, ¶ 13.

[96] GDPR, *supra* note 1, art. 7(4).

[97] *Guidelines on Consent*, *supra* note 55, ¶¶ 25–41.

[98] GDPR, *supra* note 1, art. 7(3).

From the perspective of the system's users, TechGuard would prefer a lawful basis for processing that did not grant either an *ex-ante* or *subito* "opt-out" option to the data subject. Furthermore, there are some scenarios when consent itself, although properly provided, may be insufficient. One example would be if TechGuard is a consumer ISP. It is likely that not all domestic users of each subscriber's account specifically consented to ACME Cyber Sentinel processing their data.[99] As such, it is important to explore alternative legal bases for processing the data subject's personal data.

4. Transfers

The GDPR also encompasses requirements regarding international data transfers.[100] Under the GDPR, a transfer of personal data of an EU citizen or legal person to process it outside the EU can occur "only if" the legal requirements under Chapter V of the GDPR are met.[101] If these legal requirements are not met, then a company's transfer of this data to a country outside of the EU is unlawful.[102] This Paper will explore two variations of the scenarios. In the first variation, ACME Cyber Sentinel and its clients (including TechGuard) are EU-based; the issue of transfers will have no application. For the second variation, ACME Cyber Sentinel is non-EU-based; thus, ensuring that transfers comply with the legal requirements of the GDPR can present a complex set of challenges. In the second variation, the Paper will also consider the impacts when one or more of ACME Cyber Sentinel's clients are outside the EU.

While the term "transfer" is not defined in the GDPR, the EDPB provides guidance on three criteria to identify a transfer: (1) an exporter (either a controller or a processor) is subject to the GDPR regarding the processing of personal data; (2) the exporter makes personal data available, through processing, to the importer (again, either a controller or a processor); and (3)

---

[99] For example, family members or visitors who use the WiFi may not have given their consent to TechGuard to process their data. *See Guest WiFi Advertising vs. GDPR: What You Need to Consider*, SPACE COAST DAILY (Apr. 6, 2024), https://spacecoastdaily.com/2024/04/guest-wifi-advertising-vs-gdpr-what-you-need-to-consider/ [https://perma.cc/PC9Y-SJFU]; Alex Jinks, *4 Tips for Making Guest Wi-Fi Compliant with New Privacy Laws*, SAGENET (Jan. 2020), https://www.sagenet.com/insights/4-tips-for-making-guest-wi-fi-compliant-with-new-privacy-laws/ [https://perma.cc/42DV-GQJQ].

[100] GDPR, *supra* note 1, art. 3.

[101] EDPB, *Guidelines 05/2021 on the Interplay Between the Application of Article 3 and the Provisions on International Transfers as Per Chapter V of the GDPR* ¶¶ 7–21 (Feb. 14, 2023), https://www.edpb.europa.eu/system/files/2023-02/edpb_guidelines_05-2021_interplay_between_the_application_of_art3-chapter_v_of_the_gdpr_v2_en_0.pdf [https://perma.cc/BR9H-KHFH] [hereinafter *Guidelines on Chapter V of the GDPR*]; *see* Gretchen Scott et al., *EDPB Defines a 'Transfer' Under the GDPR*, GOODWIN PROCTOR LLC (Dec. 2, 2021), https://www.goodwinprivacyblog.com/2021/12/02/edpb-defines-a-transfer-under-the-gdpr/ [https://perma.cc/V76X-9M4R].

[102] GDPR, *supra* note 1, art. 44; *see id.* at 19.

the importer is in a country outside of the EU referred to as a "third country"—regardless of whether the importer is subject to the GDPR.[103]

The GDPR's "third country" designation requires several layers of analysis, as the term applies when the country does not fall into other defined categories. Along with permitting the free flow of personal data between EU Member States, the GDPR also allows this free flow of data to members of the European Economic Area ("EEA"), which includes Iceland, Liechtenstein, and Norway.[104] Next, EU personal data can freely flow from the EU to certain countries because the European Commission has determined that these countries provide protections that are "essentially equivalent" to those provided in the EU.[105] An initial threshold for an adequacy decision appears to involve assessing whether the country's government upholds democratic principles and has an established rule of law.[106] At the time of writing this Paper, the following have received full adequacy decisions: Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, South Korea, Switzerland, the United Kingdom, and Uruguay.[107] Canada also has a limited adequacy decision related to commercial organizations.[108] As of 2023, the United States has a limited adequacy decision related to "commercial organizations participating in the

---

[103] *See generally Guidelines on Chapter V of the GDPR*, *supra* note 101.

[104] GDPR, *supra* note 1, art. 1; *see Communication from the Commission to the European Parliament and the Council: Guidance on the Regulation of a Framework for the Free Flow of Non-Personal Data in the European Union*, at 2, COM (2019) 250 final (May 29, 2019).

[105] GDPR, *supra* note 1, art. 45; *see* Maximillian Schrems v. Data Protection Comm'r, Case C-362/14, ¶ 64 (Oct. 6, 2015) (*Schrems I*); Data Protection Comm'r v. Facebook Ireland & Schrems, Case C-311/18, ¶ 120, 188 (July 16, 2020) (*Schrems II*).

[106] For example, a recent European report stated:

> The country report on the People's Republic of China (PRC) gives context to the Chinese legal system. It is held that the PRC is not a democratic, liberal state, nor does it have a rule of law. Therefore, it cannot be considered as having the ability to provide people with the protection of personal data equivalent to the EU.

EDPB, *Government Access to Data in Third Countries*, at 1 (Nov. 2021), https://edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf [https://perma.cc/7J3X-PXAN].

[107] *Adequacy Decisions: How the EU Determines if a Non-EU Country has an Adequate Level of Data Protection*, EUR COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en [https://perma.cc/KYW2-BR69] (last visited June 25, 2024) [hereinafter *Adequacy Decisions*].

[108] *Id.*; *see* Constantine Karboaliotis & Abigail Dubiniecki, *'Schrems II': Impact on Data Flows with Canada*, IAPP (Aug. 14, 2020), https://iapp.org/news/a/schrems-ii-impact-on-data-flows-with-canada/.

EU-U.S. Data Privacy Framework."[109] When a country does not fall into any of these defined categories, it is deemed a "third country," and stricter requirements apply to transfers of personal data.[110] This means that the vast majority of countries are viewed as third countries in the eyes of the EU legal system.

Transfers to third countries are permitted only where the transfer is subject to "appropriate safeguards" or if a "derogation" applies.[111] The term "appropriate safeguards" includes methods approved under Chapter V of the GDPR, including standard contractual clauses ("SCCs") and binding corporate rules ("BCRs"). For SCCs, a company contractually promises to comply with EU law and submit to the supervision of a DPA, which are independent regulators that focus on data protection in each of the EU Member States.[112] BCRs provide that a multinational company can transfer data between countries, including among affiliated entities, *after certification* of its practices by a DPA.[113] A *derogation* is akin to an exception to the normal rules, appropriate in a specific set of circumstances that occur infrequently.[114] Importantly, a derogation may apply when personal data is necessary to perform the contract between the company and the individual.

---

[109] *Adequacy Decisions*, *supra* note 107; *see* Lisa Thomas, *EU Adopts Adequacy Decision for EU-U.S. Data Privacy Framework*, NAT'L. L. REV. (July 10, 2023), https://www.natlawreview.com/article/eu-adopts-adequacy-decision-eu-us-data-privacy-framework [https://perma.cc/Y6Y2-QDX5].

[110] *Schrems I*, Case C-362/14 ¶ 122–49.

[111] "As controllers for the processing of personal data, EU institutions, bodies, offices and agencies (EUIs) are accountable for the transfers of personal data that they make and that are carried out on their behalf within and outside the European Economic Area (EEA: EU Member States and Iceland, Liechtenstein and Norway)." *International Transfers*, EUR. DATA PROTECTION SUPERVISOR https://www.edps.europa.eu/data-protection/data-protection/reference-library/international-transfers_en [https://perma.cc/FW72-KPFF] (last visited Aug. 23, 2024).

[112] *Standard Contractual Clauses (SCC)*, EUR. COMM'N, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en [https://perma.cc/A6FT-NAW2] (last visited June 25, 2022).

[113] GDPR, *supra* note 1, art. 47; *see Binding Corporate Rules (BCR)*, EUR. COMM'N, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en [https://perma.cc/R9K8-PDC7] (last visited June 25, 2024); *What are Data Protection Authorities (DPAs)?*, *supra* note 85.

[114] GDPR, *supra* note 1, art. 49. The EDPB and other EU regulators have interpreted the scope of these derogations relatively narrowly, prohibiting routine transfers under the derogations and permitting use of a derogation only where "strictly necessary." EDPB, *Guidelines 2/2019 on the Processing of Personal Data Under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects*, at 8, n.19 (Oct. 8, 2021), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf [https://perma.cc/N2X8-U5LG]; *see* Valsts Policijas Rigas Regiona Parvaldes Kartibas Policijas

When two court cases from the CJEU invalidated previous agreements between the EU and the United States, another layer of complexity was added to transfers to third countries. In the 2015 case *Schrems v. Data Protection Commissioner* ("*Schrems I*"), the CJEU struck down the Safe Harbor program, which provided a lawful basis for EU data to be transferred to the United States.[115] This decision was made in significant part based on concerns about United States government surveillance.[116] In 2020, the CJEU in *Data Protection Commissioner v. Facebook Ireland & Schrems* ("*Schrems II*") struck down the Privacy Shield—the successor agreement to the EU-U.S. Safe Harbor.[117] In *Schrems II*, the CJEU again raised concerns about the perceived lack of legal protections from United States government surveillance for EU data being transferred to the United States—specifically to Facebook, which is headquartered in the United States.[118]

In 2023, the EU provided final approval to the EU-U.S. Data Privacy Framework, the third agreement concerning EU-U.S. data flows.[119] Many expect that parties will challenge the EU-U.S. Data Privacy Framework as insufficient in the EU legal system.[120] So, transfers of personal data to the United States might once again be subject to legal uncertainty.

Parvalde v. Rigas Pasvaldibas SIA "Rigas Satiksme," Case-13/16, ¶ 30, Augstākā Tiesa [Supreme Court of the Republic of Latvia] May 4, 2017.

[115] *See Schrems I*, Case C-362/14; *see* Aurélie Pols, *The Story Behind Safe Harbor and Privacy Shield*, PIWIK (July 24, 2017), https://piwik.pro/blog/safe-harbor-privacy-shield/ [https://perma.cc/C5ZP-EEHT]; Bret Cohen & Eduardo Ustaran, *Navigating from Safe Harbor to Privacy Shield: A Primer*, HOGAN LOVELLS (July 28, 2016), https://www.engage.hoganlovells.com/knowledgeservices/news/navigating-from-safe-harbor-to-privacy-shield-a-primer/ [https://perma.cc/8KUA-5PHD].

[116] *Schrems I*, Case C-362/14 ¶¶ 11–14.

[117] In *Schrems II*, the European Court of Justice criticized the United States legal system as lacking individual redress and proportionality with regard to government surveillance practices. Data Protection Comm'r v. Facebook Ireland & Schrems, Case C-311/18, High Court, Ireland, July 16, 2020 (*Schrems II*); *see* Théodore Christakis, *After* Schrems II*: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe*, EUR. L. BLOG (July 21, 2020), https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/ [https://perma.cc/QH5A-9JTZ]. Peter Swire, one of the authors, was an expert witness in the *Schrems II* trial in Ireland. *Professor Peter Swire Testimony in Irish High Court Case*, ALSTON & BIRD, https://www.alston.com/en/resources/peter-swire-irish-high-court-case-testimony [https://perma.cc/6V7X-DJ9V] (last visited Sept. 23, 2024).

[118] *See Schrems II*, Case C-311/18.

[119] *High Court Permits Privacy Campaigner to Participate in Meta's Challenge to Data Transfer Suspension*, IRISH TIMES (Feb. 15, 2024, 4:28 PM), https://www.irishtimes.com/business/2024/02/15/high-court-permits-privacy-campaigner-to-participate-in-metas-challenge-to-data-transfer-suspension/ [https://perma.cc/PE6A-EZK5].

[120] *Id.*; Foo Yun Chee, *EU Seals New U.S. Data Transfer Pact, But Challenge Likely*, REUTERS (July 10, 2023, 2:00 PM), https://www.reuters.com/technology/eu-

Although *Schrems II* involved a U.S.-based company, the language of the case states that the decision applies generally to all third countries—with potentially significant limits on transfers to other countries outside of the EU, such as India and China.[121] For these third countries, the CJEU in *Schrems II* explicitly imposed conditions on the use of SCCs as the legal basis of transfer and implicitly raised similar concerns about the use of BCRs.[122] As *Schrems II* addressed government surveillance practices, the CJEU pointed out that the contractual nature of SCCs "cannot bind the public authorities of third countries."[123] According to *Schrems II*, "where the law of that third country allows its public authorities to interfere with the rights of the data subjects to which that data relates[,]" then data controllers must ensure that the SCCs are accompanied by "supplementary measures" to provide a "contractual guarantee of an adequate level of protection against access by the public authorities of that third country to that data."[124] Without such "adequate additional measures to guarantee such protection," *Schrems II* instructs the controller to "suspend or end the transfer of personal data to the third country concerned."[125]

5. Rights of Data Subjects/Individuals

Rights of individuals potentially relevant to this Paper are the right to object, the right to erasure, the right to data portability, and the right against automated decision-making.[126]

---

announces-new-us-data-transfer-pact-challenge-ahead-2023-07-10/ [https://perma.cc/KTG3-E2Z3].

[121] *Schrems II,* Case C-311/18 ¶ 101; *Government Access to Data in Third Countries*, *supra* note 106, at 10; Peter Swire, *The U.S., China, and Case 311/18 on Standard Contractual Clauses*, EUR. L. BLOG (July 15, 2019), https://europeanlawblog.eu/2019/07/15/the-us-china-and-case-311-18-on-standard-contractual-clauses/ [https://perma.cc/24Q4-QJET].

[122] *Schrems II*, Case C-311/18 ¶¶ 122–49; *see* Joshua P. Meltzer, *The Court of Justice of the European Union in* Schrems II*: The Impact of GDPR on Data Flows and National Security*, BROOKINGS (Aug. 5, 2020), https://www.brookings.edu/articles/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/ [https://perma.cc/QQR3-3BNF].

[123] *Schrems II*, Case C-311/18 ¶ 127.

[124] *Id.* ¶¶ 126, 133, 135.; *see* THÉODORE CHRISTAKIS, THE 'ZERO-RISK' FALLACY: INTERNATIONAL DATA TRANSFERS, FOREIGN GOVERNMENTS' ACCESS TO DATA AND THE NEED FOR A RISK-BASED APPROACH (2024).

[125] *Schrems II*, Case C-311/18 ¶ 135.

[126] *See* Jackson, *supra* note 24, at 191; *see generally* Aleksandr Kesa & Tanel Kerikmae, *Artificial Intelligence and the GDPR: Inevitable Nemeses*, 10 TALTECH J. EUR. STUDIES 68 (2020); Tiago Cabral, *Forgetful AI: AI and the Right to Erasure under the GDPR*, 6 EUR. DATA. PROT. L. REV. 378 (2020).

a. Right to Object

The right to object allows data subjects to require controllers to stop processing their personal data.[127] When a data subject objects to the processing of their personal data for direct marketing purposes, a controller must cease all such processing, including any related profiling activities.[128] Data subjects may also object to the processing of personal data based on one of the following legal bases: (1) a task carried out in the public interest, (2) the exercise of official authority, or (3) a legitimate interest; however, these objections do not trigger an absolute right.[129] In these circumstances, data subjects must provide reasons as to why they are objecting to the processing, and controllers may refuse to act on the request if they have compelling legitimate grounds overriding those of the data subject or the processing is necessary for the establishment, exercise or defense of legal claims.[130]

Data subjects, however, do not have a *de facto* veto to prevent the controller from processing their data, merely because they do not want to the controller to do so. Article 21 of the GDPR grants a right for the data subject to object to the processing of the data.[131] As mentioned above, for direct marketing and associated profiling activities, the controller must stop processing the data subject's data upon objection.[132] For other objections (like those listed in the previous paragraph), the controller must consider the data subject's objection and stop processing their data unless the controller has compelling, legitimate grounds for processing their data, which override the interests, rights, and freedoms of the data subject.[133] In short, so long as the controller has a legitimate basis for processing the personal data, and this basis is unrelated to direct marketing, the controller can continue to process the personal data if they can justify why such processing is required. The controller will need a compelling reason to override the wishes of the data subject, and this reason will be assessed *ex post* by a DPA or the European

---

[127] GDPR, *supra* note 1, art. 21.

[128] *Id.*; *id.* at 13–14; Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (Oct. 3, 2017); *What Happens if Someone Objects to My Company Processing Their Personal Data?*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/what-happens-if-someone-objects-my-company-processing-their-personal-data_en [https://perma.cc/63WU-ABJM] (last visited June 25, 2024).

[129] *Right to Object*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-object/ [https://perma.cc/ZYC9-DNF2] (last visited June 25, 2024).

[130] GDPR, *supra* note 1, art. 21; *id.* at 13–14.

[131] *Id.* art. 21.

[132] *Id.* art. 21(3).

[133] *Id.* art 21(1).

Courts on appeal.[134] This is discussed in more detail in Part.III.A.5.b, the "right to erasure."

According to *RW v Öesterreichische Post AG,* data subjects have a *de jure* right to know if a controller or processor has processed their data.[135] From the perspective of ACME Cyber Sentinel, however, it is perhaps more interesting to examine whether there is a proactive obligation placed upon the company (which we examine as a possible joint controller for this inquiry related to identifying new cybersecurity threats or training the algorithms used in these cybersecurity tools)[136] to inform the data subject that it has processed their data. This Article discussed the data controller's obligation to ensure the "transparent" processing of a data subject's data,[137] which requires the data subject's reasonable awareness that their data was processed by the controller. "Reasonableness" would be a subjective test applied *ex post* by either the relevant DPA or a court.

The first question is *how* did ACME Cyber Sentinel come into possession of the personal data? If the data was supplied to ACME Cyber Sentinel by another controller, who included the details of ACME Cyber Sentinel and its processing activities in their agreement with the data subject, then the transparency requirements are likely met.[138] However, if ACME Cyber Sentinel obtained the data subject's personal data through some other means, such as from a dump of compromised account data on the dark web where the data subject is uninformed about ACME Cyber Sentinel, ACME Cyber Sentinel will likely need to proactively inform the data subject of its collection and processing of their personal data to comply with the transparency obligations. Again, while the data subject has a right to object to the processing of their data, this right is not automatic in the context of the operation of ACME Cyber Sentinel's data processing as it is not direct marketing. Also, if ACME Cyber Sentinel has a compelling and legitimate basis for processing the personal data of the data subject, notification of processing would likely not to be a barrier to continued processing of the personal data.

---

[134] This process has been demonstrated in UF & AB v. Land Hessen. Joined Cases C-26/22, C-64/22, UF & AB v. Land Hessen, 2023, and it was noted that where there are such legitimate grounds, these may be determined by the courts even if not put forward by the controller.

[135] RW v. Österreichische Post AG, Case C-154/21, Oberster Gerichtshof [OGH] [Supreme Court] Jan. 12, 2023.

[136] In Part IV.B.2, we discuss under which circumstances ACME Cyber Sentinel may be acting as a joint controller. If ACME Cyber Sentinel is a processor, then it would not be responsible for addressing the individual rights of data subjects; that requirement would fall to the controller.

[137] GDPR, *supra* note 1, art. 5(1)(a).

[138] *RW*, C-154/21 ¶¶ 34–35.

b. Right to Erasure

Under Article 17 of the GDPR, the data subject can request that the controller erase their personal data when certain conditions are met.[139] The first of these conditions is straightforward: once the data subject believes the controller or processor no longer requires their personal data for the processing purposes, the data subject can request the data's erasure.[140] The second condition is also straightforward as it arises when the data subject has withdrawn consent for processing their data, and the controller has relied on that consent as the lawful basis for processing their personal data.[141] Revocation of consent allows the data subject to request deletion of their data. However, it is unlikely that ACME Cyber Sentinel will rely on consent as a lawful means of processing personal data obtained from TechGuard.[142]

Suppose ACME Cyber Sentinel has used either "legitimate interests" or "public interest" as a lawful means of processing. In that case, the data subject has a right to object to the processing under Article 21(1) of the GDPR. However, if ACME Cyber Sentinel has no overriding legitimate grounds to continue processing their personal data, the data subject can seek to have that personal data erased pursuant to Article 17(1)(c). As has already been discussed in this Paper, the CJEU views processing data for cybersecurity purposes as a valid, legitimate interest.[143] ACME Cyber Sentinel will need to demonstrate why this interest overrides the data subject's objection to processing the data.

Erasure can also be sought by the data subject if their personal data has been processed unlawfully[144] or if an EU Member State's law requires the deletion of their data.[145] Furthermore, as the CJEU clarified in *Budapest*,[146] a supervisory authority can compel the controller to erase a data subject's personal data, even when the data subject themselves has not requested the data's erasure.[147] *Budapest* also confirmed that, in the event of unlawfully processed personal data, the supervisory authority can compel the personal

---

[139] These conditions are outlined in articles 17(1)(a)–(f). GDPR, *supra* note 1, arts. 17(1)(a)–(f).

[140] GDPR, *supra* note 1, art. 17(1)(d).

[141] *Id.* art. 17(1)(b).

[142] *See supra* Part III.A.3.

[143] Meta Platforms v. Bunde Meta Platforms v Bundeskartellamt, Case C-252/21, Bundesgerichtshof [BGH] [Higher Regional Court, Düsseldorf, Germany] July 4, 2023; *see* GDPR, *supra* note 1, at 9 ("The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security . . . constitutes a legitimate interest of the data controller concerned.").

[144] GDPR, *supra* note 1, art. 17(1)(d).

[145] *Id.*

[146] Budapest Főváros IV. Kerület Újpest Önkormányzat Polgármesteri Hivatala v. Nemzeti Adatvédelmi és Információszabadság Hatóság, Case C-46/23, Fővárosi Törvényszék [Budapest High Court, Hungary] Mar. 14, 2024.

[147] *Id.* ¶ 48.

data's erasure even when the controller has obtained the personal data from sources other than the data subject.[148]

Under Article 17(3) of the GDPR, the controller can challenge an erasure request by using one of the exceptions listed in Article 17(1)(a)–(f); however, these exceptions are both comprehensive and final.[149] From the perspective of ACME Cyber Sentinel, exception (d) is of particular interest as it is an exception where the controller has relied on Article 89 of the GDPR with regard to data processing. To succeed in using this exception, however, the controller must demonstrate how the erasure of this particular personal data will seriously impair or render impossible the scientific research that they are conducting.[150]

Article 17's consequences for ACME Cyber Sentinel are that the company must have a policy that handles the removal of personal data once it is no longer relevant for the original processing purposes.

c. Right to Prevent Automated Decision-Making

Article 22(1) of the GDPR provides a data subject "the right to not be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[151] Could the data subject, therefore, opt out of having their personal data processed by ACME Cyber Sentinel under any of the scenarios?

The CJEU examined this right in the recent case of *QQ v. Land Hessen*.[152] In *QQ*, an individual challenged the production of an automatically calculated credit score made available to financial institutions.[153] For Article 22(1) to apply, the CJEU stated that a three-part test must be satisfied: (1) there must be a decision; (2) the result must have been based solely on automated processes; and (3) the consequences of the decision must produce legal effects regarding the individual, or alternatively produce similarly significant effects.[154] Accordingly, if the consequences of ACME Cyber Sentinel's assessment of an individual's personal data were to produce significant impacts on the data subject, such as denying them internet access or denying them the ability to access banking or governmental internet resources, then the consequences of the decision could be sufficient to invoke Article 22(1).[155]

---

[148] *Id.* ¶ 53.

[149] GDPR, *supra* note 1, arts. 17(3)(a)–(e).

[150] *Id.* art. 17(3)(d).

[151] *Id.* art. 22(1).

[152] OQ v. Land Hessen, Case C-634/21 [Verwaltungsgericht Wiesbaden] Dec. 7, 2023.

[153] *Id.* ¶¶ 14–17.

[154] *Id.* ¶ 43.

[155] *See* GDPR, *supra* note 1, art. 22(1).

There is a view within legal academia that Article 22(1) represents a *de facto* prohibition on automated decision-making that produces legal or equivalent effects in the absence of additional protections,[156] and the referring court appeared to take this view of Article 22(1) in the oral arguments of *QQ*.[157] The CJEU's judgment suggests that it may also take this position. The opinion of the Advocate General, which views Article 22(1) as a prohibition, is referenced in the judgment.[158] To enable processing as outlined in Article 22(1),[159] the CJEU also states that one of the conditions in Article 22(2) must be present.[160] Specifically, the processing must either be required to perform a contract authorized under a specific EU law or based on the data subject's consent.[161]

Therefore, in accordance with *QQ*, ACME Cyber Sentinel must carefully review the consequences of the personal data assessment as requested by TechGuard to ensure that they are not so significant that Article 22(1) applies.

B. EU AI Act

The newly enacted EU AI Act, which is designed to work in tandem with the GDPR, focuses on the technical development and uses of AI systems. The EU AI Act is based on a risk categorization system, requiring different obligations for the various AI risk categories.[162] The risk categories are as follows: unacceptable risk AI systems, high-risk AI systems, and low-risk AI

---

[156] *See, e.g.*, Florent Thouvenin et al., *Article 22 GDPR on Automated Individual Decision-Making: Prohibition or Data Subject Right?*, 8 EUR. DATA PROT. L. REV. 183 (2022); see also Christian Djeffal, *The Normative Potential of the European Rule on Automated Decisions: A New Reading for Art. 22 GDPR*, 81 Z. AUSLANDISCHES OFFENTLICHES RECHT VOLKERRECHT 847 (2020), for a more detailed discussion of this proposal.

[157] Andreas Häuselmann, *The ECJ's First Landmark Case on Automated Decision-Making – a Report From The Oral Hearing Before the First Chamber*, EUR. L. BLOG (Feb. 20, 2023), https://europeanlawblog.eu/2023/02/20/the-ecjs-first-landmark-case-on-automated-decision-making-a-report-from-the-oral-hearing-before-the-first-chamber/ [https://perma.cc/CWB6-9TPZ].

[158] *OQ v. Land Hessen*, Case C-634/21 ¶ 52.

[159] *Id.* ¶¶ 53–54.

[160] *Id.*

[161] *Id.*

[162] EU AI Act, *supra* note 2; *see* James Clark et al., *Europe: The EU AI Act's Relationship With Data Protection Law: Key Takeaways*, DLA PIPER (Apr. 25, 2024), https://privacymatters.dlapiper.com/2024/04/europe-the-eu-ai-acts-relationship-with-data-protection-law-key-takeaways/ [https://perma.cc/B3EV-J876]; Andrew Folks, *EU AI Act 101*, IAPP (Mar. 2024), https://iapp.org/media/pdf/resource_center/eu-ai-act-101-chart.pdf [https://perma.cc/G853-TM77]; Odia Kagan, *In Scope or Not? An EU AI Act Decision Tree and Obligations*, IAPP (Jun. 14, 2023), https://iapp.org/news/a/in-scope-or-not-an-eu-ai-act-decision-tree-and-obligations/ [https://perma.cc/U6KJ-GWF3].

systems.[163] The unacceptable risk AI systems are prohibited in the EU, such as "emotion recognition systems" at work or in school that identify or infer "emotions or intentions" of individuals based on biometric data.[164] High-risk AI systems relate to decisions made concerning health, safety, or fundamental rights, such as emotion recognition systems, medical devices, vehicles, and law enforcement."[165] As one would expect, high-risk AI systems are the most regulated of the permitted AI systems, with a list of obligations including an enumerated cybersecurity requirement.[166] Low-risk AI systems, those that present minimal or no risk to rights or safety, are expected to inform individuals that they are interacting with an AI system and can voluntarily adhere to industry codes of conduct.[167]

AI systems utilized in cybersecurity are not likely to fall into the unacceptable risk category of the EU AI Act. As to high-risk AI systems, cybersecurity AI systems would not appear to generate the types of decisions, such as those related to fundamental rights, that lead to designation as high risk under the EU AI Act.[168]

Due to the recent implementation of the EU AI Act, many questions have been left unanswered and minimal scholarship clarifies how it applies to cybersecurity companies.[169] AI is crucial to state-of-the-art cybersecurity; therefore, this Paper's analysis seeks to raise awareness of potential concerns.

---

[163] General-purpose AI models are also governed under the EU AI Act. EU AI Act, *supra* note 2.

[164] *Id.* art. 5(1)(f); *see id.* arts. 3(34) & 3(39); *see* also William Fry, *The Time to (AI) Act is Now: A Practical Guide to Emotion Recognition Systems Under the AI Act*, LEXOLOGY (July 19, 2024), https://www.lexology.com/library/detail.aspx?g=eeb232b8-4bb8-49d8-94a0-15341834193e [https://perma.cc/VJ7E-F6U9]; *High-Level Summary of the AI Act*, EU ARTIFICIAL INTELLIGENCE ACT (Feb. 27, 2024), https://artificialintelligenceact.eu/high-level-summary/ [https://perma.cc/9K9Q-XPAC].

[165] EU AI Act, *supra* note 2, art. 6(2); *see id.* at 127–29; *see* Anna-Lena Kempf & Nils Rauer, *A Guide to High-Risk AI Systems Under the EU AI Act*, PINSENT MASONS (Feb. 13, 2024), https://www.pinsentmasons.com/out-law/guides/guide-to-high-risk-ai-systems-under-the-eu-ai-act [https://perma.cc/QTG2-A7CN].

[166] EU AI Act, *supra* note 2, ¶ 74.

[167] EU AI Act, *supra* note 2, at 82–83; see Kaitlyn E. Stone & Michael C. Zogby, *AI Coming to the EU: EU Artificial Intelligence Act's Recent Publication, Next Steps*, BARNES & THORNBURG LLP (Aug. 1, 2024), https://btlaw.com/insights/alerts/2024/ai-coming-to-the-eu-eu-artificial-intelligence-acts-recent-publication-next-steps [https://perma.cc/ZHD2-PKL2].

[168] *See* EU AI Act, *supra* note 2, at 126–29.

[169] *See* Federica Casarosa, *The Risk of Unreliable Standards: Cybersecurity and the Artificial Intelligence Act*, INTERNET POL'Y REV. (Feb. 29, 2024), https://policyreview.info/articles/news/cybersecurity-and-artificial-intelligence-act/1742 [https://perma.cc/X4KM-KTHP]; *see also Entry Into Force of the European AI Regulation: The First Questions and Answers from the CNIL*, CNIL (July 12, 2024), https://www.cnil.fr/en/entry-force-european-ai-regulation-first-questions-and-answers-cnil [https://perma.cc/FCE7-G6N4].

IV. LEGAL PRINCIPLES APPLIED TO SCENARIOS

This Paper now applies the applicable legal principles to each of the scenarios introduced in Part II. Our approach is to examine ACME Cyber Sentinel's legal requirements, operating under the assumption that the company seeks to comply with the applicable requirements. This analysis also considers that context is typically crucial for cybersecurity. ACME Cyber Sentinel will often need to establish a baseline, such as a baseline of user activity, to distinguish between acceptable activities and malicious activities.[170] In these scenarios, ACME Cyber Sentinel is carrying out its activities for TechGuard, so the GDPR applies to the data protection concerns for any personal data.[171]

Under the GDPR, different entities can carry out the processing of personal data under a hierarchy of responsibility. At the top of the hierarchy lies the data controller,[172] whilst beneath the controller is a data processor.[173] Although the relationship between the controller and processor is not always clear cut, the processor has fewer responsibilities than the controller.

In these scenarios, TechGuard is a controller of the data from its customers and its employees. Because the legal framework created by the GDPR allows for joint controllers, one of the inquiries critical to each scenario is whether ACME Cyber Sentinel is acting as a processor or a controller; the answer will dictate the range of responsibilities that ACME Cyber Sentinel will face regarding the personal data it is processing from TechGuard. When examining these roles, it is important to remember that the determination of whether an entity is a processor or a controller is not based on the nature of the entity (such as a cybersecurity service provider); instead, it is a fact-specific inquiry. The decision is based on the activities of the entity in a specific situation, meaning the entity's role needs to be assessed with regard to each processing activity undertaken. This means ACME Cyber Sentinel can be determined to be a processor in certain of the scenarios presented in this Paper and a controller in other scenarios.

---

[170] *See* Jackson, *supra* note 24, at 183.

[171] If ACME Cyber Sentinel were to carry out its activities on behalf of the European Commission (or another European agency), the public sector counterpart will be the relevant legislation. Processing of personal data by European Institutions and agencies is not covered under the GDPR, but instead under a distinct 'public sector' counterpart of the GDPR. *See* GDPR, *supra* note 1, ¶ 154. Law enforcement processing of data is not covered by the GDPR. *See* Directive on the Protection of Natural Persons, *supra* note 80. It is important to note that while the GDPR is a regulation, and therefore the text of the regulation is directly applicable and uniform across every Member State, the Law Enforcement directive is a directive, and so the specific text may vary from Member State to Member State. However, the text of the Directive will act as a minimum set of data protection requirements for law enforcement activities. *Id.*

[172] GDPR, *supra* note 1, art. 4(7).

[173] *Id.* art. 4(8).

In an effort to achieve compliance with EU legal requirements, the analysis here assumes that ACME Cyber Sentinel initially undertakes measures to protect client data. Specifically, ACME Cyber Sentinel collects and transfers the minimum amount of data for ML training purposes as required by GDPR's data minimization principles. Before transferring data across borders, ACME Cyber Sentinel anonymizes personal data and any sensitive data to mitigate privacy risks, whenever such actions do not conflict with the data's cybersecurity needs. In addition, ACME Cyber Sentinel is transparent in communicating with its clients about the use of their data for ML training.

We examine two different variations for each of these scenarios. Initially, we assume that both TechGuard and ACME Cyber Sentinel are based in the EU, which underscores the importance of addressing potential regulatory challenges and data privacy concerns by focusing on the requirements when TechGuard and ACME Cyber Sentinel are located in the same jurisdiction. In alternate versions of these scenarios, ACME Cyber Sentinel is based outside the EU. This analysis will highlight additional complexities that arise when TechGuard and ACME Cyber Sentinel are *not* headquartered in the same jurisdiction.

A. Analysis for Scenario 1

Scenario 1 focuses on ACME Cyber Sentinel providing cybersecurity services to TechGuard. The questions for this scenario are: Is ACME Cyber Sentinel a processor or a controller? Does ACME Cyber Sentinel access the data considered personal data? What is the lawful basis for ACME Cyber Sentinel to process this data? Can the personal data be transferred to ACME Cyber Sentinel?

1. Is ACME Cyber Sentinel a processor or a controller?

As noted, a controller has numerous legal obligations under the GDPR. In these scenarios, and as mentioned above, TechGuard is a controller of the data from its customers and its employees. It is important to remember that the legal framework created by the GDPR allows for more than one controller of the data in a particular transaction involving data—referred to as joint controllers. The critical inquiry to this scenario is whether ACME Cyber Sentinel is acting as a processor or a controller when it provides cybersecurity-related services to TechGuard.

In this scenario, ACME Cyber Sentinel is a processor. Under EU law, a processor is an entity that undertakes "process[ing] personal data on behalf of the controller."[174] The term "on behalf of" invokes the legal concept of delegation—where specific tasks are carried out by the processor based on the controller's instructions regarding the purposes and means of processing the

[174] *Id.* art. 4(8); *see Guidelines on the Concepts of Controller and Processor*, *supra* note 57, ¶ 76.

personal data.[175] In the controller-processor relationship, the processor has a "certain degree of discretion" regarding how to best carry out the instructions of the controller, particularly with regard to selecting "the most suitable technical and organisational means."[176]

In drawing the line between the choices within the discretion of the processor and the judgments that are reserved to the controller, a processor is permitted to exercise its discretion with regard to the more practical aspects of implementation of the controller's instructions—known as the "non-essential means."[177] In its guidelines on controllers and processors, the EDPB states that "the detailed security measures based on the general security objectives set by the other party"[178] are considered "non-essential means."[179] Because ACME Cyber Sentinel undertakes the processing of personal data to provide cybersecurity services, its cybersecurity decisions would fall into the category of "non-essential means"—supporting a conclusion that ACME Cyber Sentinel is acting in the role of a processor for the processing activity in Scenario 1.

In examining the services provided by ACME Cyber Sentinel, it is worth examining the fact that a processor typically engages in "processing personal data *on the controller's behalf*."[180] For companies that provide cybersecurity services, the processing of personal data is generally *not* the main focus of their services. On this point, the EDPB initially states:

> In practice, where the provided service is not specifically targeted at processing personal data or where such processing does not constitute a key element of the service, the service provider may be in a position to independently determine the purposes and means of that processing which is required in order to provide the service.[181]

---

[175] *Guidelines on the Concepts of Controller and Processor*, *supra* note 57, ¶ 80; *id.* ¶ 34; *see* GDPR, *supra* note 1, art. 4(7).

[176] *Guidelines on the Concepts of Controller and Processor*, *supra* note 57, ¶ 80.

[177] *Id.* ¶¶ 39–41.

[178] In the flowchart provided by the EDPB on practically determining status as a processor or controller, an entity is asked whether it decides the purpose of processing. *Id.* at 49. A processor would answer: "No, I carry out the processing on behalf of another party, in accordance with its instructions. I make decisions about certain non-essential means to be used (e.g., what IT systems or other technical means to use for the processing or details of the security measures based on the general security objectives set by the other party)." *Id.*; *see id.* ¶¶ 39–40.

[179] The processor agreement is expected to include a description of the controller's "security objectives." *Id.* ¶ 127. In certain circumstances, "the controller may describe the minimum security objectives to be achieved, while requesting the processor to propose implementation of specific security measures." *Id.*

[180] *Id.* ¶ 76

[181] *Id.* ¶ 82.

Importantly for this discussion, the EDPB then proceeds to explain that "a service provider may still be acting as a processor even if the processing of personal data is not the main or primary object of the service," so long as the client of the service determines the purposes and means of the processing.182

The EDPB provides two examples relevant to labeling companies providing cybersecurity services.[183] The first example deems a call center a processor when it provides support services to its client's customers by accessing the client's data bases—a situation where processing personal data is not the main focus of the service.[184] The second example involves a company that provides general IT support for its client, which is also described as acting in the role of a processor as processing personal data is not the main focus of the service.[185] These two examples suggest that ACME Cyber Sentinel would be acting as a processor when it provides cybersecurity services so long as TechGuard determines the purposes and means of the processing.

In Scenario 1, ACME Cyber Sentinel is likely to be a processor because TechGuard has given general instructions to ACME Cyber Sentinel to provide cybersecurity services (which is the overall purpose) while permitting ACME Cyber Sentinel to use its discretion to determine the technical means to accomplish the specific security measures. Assuming TechGuard is the sole controller in this scenario, it would remain responsible for the implementation of the non-essential technical means related to security.[186] Although ACME Cyber Sentinel would be granted discretion to determine the specific security measures used, the agreement between the two parties should ensure that

---

[182] *Id.* ¶ 83. In one example, an IT consultant is hired to fix a bug in software. *Id.* According to the example, "The IT-consultant is not hired to process personal data, and Company ABC determines that any access to personal data will be purely incidental and therefore very limited in practice." *Id.* Under this set of facts, the IT consultant is deemed to be neither a processor nor a controller. *Id.*

[183] Although none of the examples from the EDPB can be expected to cover all aspects relevant to cybersecurity, these examples can be instructive on particular points. *Id.*

[184] *Id.*

[185] "The access to personal data is not the main object of the support service but it is inevitable that the IT service provider systematically has access to personal data when performing the service." *Id.*

[186] *Id.* ¶ 41 ("Even though decisions on non-essential means can be left to the processor, the controller must still stipulate certain elements in the processor agreement, such as – in relation to the security requirement, e.g. an instruction to take all measures required pursuant to Article 32 of the GDPR. The agreement must also state that the processor shall assist the controller in ensuring compliance with, for example, Article 32. In any event, the controller remains responsible for the implementation of appropriate technical and organisational measures to ensure and be able to demonstrate that the processing is performed in accordance with the Regulation (Article 24).").

TechGuard is informed about the security measures used by ACME Cyber Sentinel to enable that TechGuard to ensure that the processing is lawful.[187]

Much of this application of the law to the facts in this scenario is based on the guidance by the EDPB, not the CJEU. The assessment relies heavily on the distinction between essential and non-essential means found in the EDPB's guidelines on controllers and processors.[188] Although the CJEU has not directly considered the issue of essential and non-essential means, it is worth noting that numerous scholars, including Orla Lynskey, Manuel Klar, and Yordanka Ivanova, have pointed out that when the courts have had the opportunity to examine the controller/processor relationship, parties have used their rulings to "stretch" the definition of the controller to ensure "complete and effective" protection of an individual's right to data privacy.[189]

---

[187] "[T]he controller must be fully informed about the [technical] means that are used so that it can make an informed decision in this regard." *Id.*; *see id.* ¶ 126. In the example of a call center that provides customer service on behalf of the client company, the client company signs a processor agreement with the call center where the client approves the technical and organizational security measures proposed by the call center. *Id.* ¶ 41. Once approved, the call center determines non-essential means of processing – such as the particular software to be used and the particular security measures to be put in place. *Id.*

[188] *See* Orla Lynskey, *Complete and Effective Data Protection*, 76 CURR. LEG. PROBL. 297, 312 n.88 (2023) ("The EDPB distinguishes between essential means of processing (which is closely linked to purposes) and includes determining what and whose personal data is processed and for long, and non-essential means which concerns more practical aspects of implementation (e.g. Hardware choices).").

[189] *See id.* at 308–13 (2013) (tracing the evolution of court decisions with regards to controllership, and noting how as we enter an environment of interconnected services and platforms, the likelihood of users finding themselves "joint controllers" increases); Klar, *supra* note 78, at 105, 138; Yordanka Ivanova, *Data Controller, Processor or a Joint Controller: Towards Reaching GDPR Compliance in the Data and Technology Driven World*, *in* PERSONAL DATA PROTECTION AND LEGAL DEVELOPMENTS IN THE EUROPEAN UNION 61, 63 (Maria Tzanou ed., 2020). One example of the courts identifying a presumed processor as a controller is the *Facebook Fanpage* case, although this decision has been met with some controversy. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH, Case C-210/16, Bundesverwaltungsgericht [Federal Administrative Court, Germany] June 5, 2018 (*Facebook Fanpage Case*). The court noted that while the mere use of a social media network, such as Facebook, does not make the user a controller, the act of creating a fan page on the social media does give Facebook the ability to place cookies on the devices of users of that fan page. *Id.* ¶ 35. Furthermore, Facebook provides the administrator of the fan page the ability to request demographic information about the users, which will result in Facebook processing the personal data of the users in order to present this information, a fact which the court held to be an example of the administrator determining the nature of the processing of the data subject's information. *Id.* ¶ 37. Even though at no stage did Facebook provide the administrator with the actual personal data of the users, the fact that the data which was provided to the administrator was derived from the processing of personal data, and the fact that the administrator was involved in the promotion of the fan page was sufficient to

Throughout its guidance, the EDPB cites to numerous CJEU decisions when it stated that "the concept of 'controller' should be interpreted in a sufficiently broad way, favoring as much as possible effective and complete protection of data subjects so as to ensure full effect of EU data protection law[.]"[190]

It is important to remember that the determination of an entity's role as a processor or controller for a particular purpose is a fact-specific inquiry. The EDPB provides examples that highlight two related issues to help differentiate between a processor and a controller: (1) whether the entity has significant independence in how to handle the personal data; and (2) whether the activity is linked to a functional role of the entity. Importantly, future developments related to cybersecurity could shift the factual-specific inquiry toward the view that a cybersecurity company, like ACME Cyber Sentinel, is acting as a controller.

First, when an entity has substantial independence in how to handle the processing of personal data, this supports the conclusion that the entity is acting as a controller. In a law firm example, the law firm has "a significant degree of independence . . . in deciding what information to use and how to use it," to provide legal representation, while the client company provides the law firm with no instructions regarding the processing of personal data for this purpose.[191] Next, a bank example examines a situation where the client company requests that the bank undertake payments to employees. Due to banking regulations, the client company is *not* permitted to have "any influence on the purpose and means" of the bank's processing of personal data to perform banking activities; this indicates that the bank is acting as a controller.[192] An accounting firm's auditing scenario examines both a controller role and a processer role. When the auditing is carried out in accordance with the legal requirements regulating the tasks involved in

---

ground their status as a controller. *Id.* ¶ 40. It must be noted that, similar to *Breyer* and *Nowak*, the relevant legislation for this case was the 1995 Data Protection Directive; however, the concept of a "controller" is virtually unchanged in the GDPR and the CJEU has recognised the authority of this case with regards to the GDPR in Facebook Ireland Ltd, Facebook Inc., Facebook Belgium BVBA v Gegevensbeschermingsautoriteit, Case C-645/19, ¶ 91, High Court, Ireland, June 15, 2021.

[190] *Guidelines on the Concepts of Controller and Processor*, *supra* note 57, ¶ 14 (citing Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV, Case C-40/17, ¶ 66 [Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany)] July 29, 2019; *Wirtschaftsakademie Schleswig-Holstein*, Case C-210/16 ¶ 28; Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Case C-131/12, ¶ 34 [Request for a Preliminary Ruling from the Audiencia Nacional of Spain] May 13, 2014)).

[191] *Id.* ¶ 27.

[192] *Id.* ¶ 40. In the flowchart meant to assess whether a company is acting as a controller, the question is posed: "Is the processing necessary in order to carry out a task for which you are responsible according to a legal act? (implicit legal compliance)." *Id.* at 49. If the answer is yes, "You are the controller of the processing necessary to execute the task." *Id.*

auditing, the accounting firm "determines what data it needs to have, which categories of persons that need to be registered, how long the data shall be kept and what technical means to use."[193] This decision-making power indicates that the accounting firm is acting as a controller.[194] In a scenario where the law does not establish the auditing requirements, then the client company provides detailed instructions for auditing; the accounting firm is more likely to be acting as a processor in this scenario.[195] In an example of payroll administration, the client company provides detailed "instructions on who to pay, what amounts, by what date, by which bank, how long the data shall be stored, what data should be disclosed to the tax authority."[196] These instructions from the client company are an indicator that the payroll administrator is providing services as a processor, even in a situation where the payroll administrator can determine non-essential processing means such as which software to use and how to distribute access to the personal data within its company.[197]

Second, when an entity engages in an activity that is linked to its functional role, this supports the conclusion that the entity is acting as a controller for the particular processing activity. In the law firm example, the purpose of processing the personal data is to represent the client in court and is "linked to the functional role" of the law firm; the "professional expertise" of a law firm in representing a client is one indicator that the law firm is acting as a controller for this purpose of processing personal data.[198] The example of an accounting firm explores two variations of a scenario where the accounting firm provides auditing services—one where the accounting firm is in the role of a controller and the other where it acts as a processor. When the auditing is carried out in accordance with the laws regulating the profession, the processing can be viewed as "part of the accounting firm's core activity," which is one indicator that the accounting firm is acting as a controller.[199] Conversely, in a scenario where the requirements for auditing are not established by law, the processing by the accounting firm is an "ancillary task that is carried out as part of the client company's activity"—meaning the accounting firm is more likely to be acting as a processor.[200]

The cybersecurity field likely faces increasing regulation related to data and growing expectations about how to provide these professional services. Today, companies providing cybersecurity services are often labeled

---

[193] *Id.* ¶ 40.

[194] *Id.* The EDPB notes, "Rather than directly appointing the controller or setting out the criteria for its appointment, the law will [more commonly] establish a task or impose a duty on someone to collect and process certain data. In those cases, the purpose of the processing is often determined by the law." *Id.* ¶ 24; *see id.* at 49.

[195] *Id.* ¶ 40.

[196] *Id.*

[197] *Id.*

[198] *Id.* ¶ 27.

[199] *Id.* ¶ 40; *see id.* at 49.

[200] *Id.* ¶ 40.

processors. Over time, however, cybersecurity companies are more likely going to be considered controllers. From a legal perspective, the CJEU has stretched the definition of controller to ensure effective protection of the right to privacy. From an industry perspective, more regulations are being enacted that cover the cybersecurity field (analogous to the banking example) and more internal expectations are being implemented in the cybersecurity industry (akin to the accounting and law firm examples). As the cybersecurity industry continues to mature and its value to the proper functioning of business technologies is highlighted, the likelihood that a company, such as ACME Cyber Sentinel, would exercise "a significant degree of independence . . . in deciding what information to use and how to use it . . . ." increases and the company is more likely to act as a controller.[201] The key inquiry here, that Scenario 2 will revisit, is whether the expertise required to provide cybersecurity services necessitates ACME Cyber Sentinel being involved in the essential means of processing, and not merely the non-essential means.

2. Is the data accessed by ACME Cyber Sentinel considered personal data?

The GDPR applies only to personal data.[202] Some information, such as IP addresses and media access control ("MAC") addresses,[203] often constitute personal data.[204] Other information, such as file names, command lines and user IDs may include personal data if used in the naming convention or if the identifier is specific to an individual, such as the only user of a specific machine or device. For the first scenario, TechGuard, rather than ACME Cyber Sentinel, determines whether personal data exists on the TechGuard systems.

Information such as indicators of compromise may be processed in a way that is not personal data. Scenario 2 will explore how this type of non-personal data could potentially transform into personal data if it combines

---

[201] *Id.* ¶ 27.

[202] GDPR, *supra* note 1, art. 1(1).

[203] John Bogna, *What is a MAC Address, and How Does it Work?*, HOW-TO GEEK (Nov. 16, 2021), https://www.howtogeek.com/764868/what-is-a-mac-address-and-how-does-it-work/ [https://perma.cc/W7JH-R3JG] ("MAC addresses are associated with specific devices and assigned to them by the manufacturer . . . MAC addresses work with the card in [the] device that lets it connect wirelessly to the internet, called a Network Interface Controller (NIC) . . . MAC addresses are always a 12-digit hexadecimal number, with the numbers separated every two digits by a colon or hyphen.").

[204] *Can We Identify an Individual Indirectly from the Information We Have (Together with other Available Information)?*, ICO, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/can-we-identify-an-individual-indirectly/?q=photograph#:~:text=MAC%20addresses%20are%20intended%20to,the%20data%20is%20personal%20data [https://perma.cc/6E9K-M83C] (last visited June 28, 2024).

with additional datasets, such as those found on the dark web after a data breach.

For phishing detection, ACME Cyber Sentinel may review the content of emails as well as the inspection of the uniform resource locators ("URLs") within the emails.[205] Such activity could potentially reveal users' "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership."[206] Cybersecurity services such as phishing detection often involves processing personal data and sometimes special categories of personal data, which may require stricter safeguards.

3. What is the lawful basis for ACME Cyber Sentinel to process this data?

Where ACME Cyber Sentinel finds itself in possession of personal data, and to the extent it acts as a controller of this personal data, ACME Cyber Sentinel must demonstrate, on an *ex-ante* basis, that it had a lawful basis to process this data for a particular purpose.[207] Under Article 6 of the GDPR, being "necessary for the performance of a contract" is one basis for lawful processing.[208] When ACME Cyber Sentinel acts as a processor for TechGuard for cybersecurity purposes, their contract may well provide the legal basis.[209] That basis may not exist, however, for special categories of personal data.

4. Can the personal data be transferred to ACME Cyber Sentinel?

In this alternative version of the scenario, ACME Cyber Sentinel is based outside of the EU. As the majority of the companies that provide CSaaS are based in the United States,[210] this first examination envisions ACME Cyber Sentinel as a company headquartered in the United States. Currently, these transfers of personal data from the EU to the United States can occur pursuant to the EU-U.S. Data Privacy Framework where the United States is treated as an adequate country for transfers of commercial data; this means that EU data

---

[205] Luz & Frank, *supra* note 18; *see* Divakaran & Oest, *supra* note 18.

[206] GDPR, *supra* note 1, art. 9(1).

[207] "Each purpose requires a separate legal ground that will legitimize the processing." Böck et al., *supra* note 43, at 13.

[208] GDPR, *supra* note 1, art. 6(1)(b).

[209] *Id*. art. 6(2)(b). Notably, there is no equivalent basis for the processing of special categories of data due to contractual necessity. Under Scenario 2, this Paper explores additional lawful basis that may apply for special categories of data.

[210] Ignacio Sbampato, *Where are the European Cybersecurity Vendors?*, CYBERHIVE (Aug. 23, 2024), https://thecyberhive.eu/community/articles/where-are-european-cybersecurity-vendors [https://perma.cc/Q6JP-BLHR]; *see also Organizational Effects*, *supra* note 5.

is permitted to flow "freely" from the EU to "U.S. certified companies."[211] In addition, U.S.-based companies can rely on either SCCs or BCRs as a lawful basis of transfer.[212]

When ACME Cyber Sentinel is headquartered in a country without an adequacy decision, such as Brazil, India, or China,[213] the relationship between TechGuard and ACME Cyber Sentinel becomes more complex.[214] As the requirements of *Schrems II* apply to third countries,[215] the burden is placed on data controllers to ensure that the SCCs (and presumably BCRs) are accompanied by "supplementary measures" to provide guarantees of "an adequate level of protection against access by the public authorities of that third country to that data."[216] In raising data privacy concerns related to government surveillance practices of foreign governments, the CJEU emphasized that the contractual nature of SCCs "cannot bind the public

---

[211] *EU-U.S. Data Privacy Framework, F.A.Q. for European Individuals,* EDPB (Jul. 16, 2024), at 3, https://www.edpb.europa.eu/system/files/2024-07/edpb_dpf_faq-for-individuals_en_0.pdf [https://perma.cc/QM2K-LL2J]; *see* Data Protection Comm'r v. Facebook Ireland & Schrems, Case C-311/18, High Court, Ireland, July 16, 2020 (*Schrems II*). Important to this discussion, many commentators expect that the EU-U.S. Data Privacy Framework will be challenged as insufficient in the EU legal system. *See* Chee, *supra* note 120. If a future challenge to this current United States adequacy decision was to invalidate the EU-U.S. Data Privacy Framework, then the United States would be viewed as a third country unless and until the United States could successfully negotiate another deal. *Id.* In two earlier instances, the CJEU has invalidated the adequacy decisions between the EU and the United States—the 2015 *Schrems I* case that invalidated the Safe Harbor and the 2020 *Schrems II* case that invalidated the Privacy Shield. *See* Maximillian Schrems v. Data Protection Comm'r, Case C-362/14, ¶ 64 (Oct. 6, 2015) (*Schrems I*)*;* Data Protection Comm'r v. Facebook Ireland & Schrems, Case C-311/18, (July 16, 2020) (*Schrems II*); Robb Hiscock, *EU-US Data Privacy Framework: A Brief History*, ONETRUST (July 12, 2023), https://www.onetrust.com/blog/eu-us-data-privacy-framework-a-brief-history/ [https://perma.cc/EC3D-QD2C]. If this occurred, it would mean that TechGuard, acting as the controller in this scenario, would need to require additional safeguards for the personal data that ACME Cyber Sentinel processes.

[212] Gretchen Scott et al., *What Companies Need to Know about the New EU-U.S. Data Privacy Framework for Cross-Border Data Transfers*, GOODWIN (July 17, 2023), https://www.goodwinlaw.com/en/insights/publications/2023/07/alerts-otherindustries-dpc-what-companies-need-to-know [https://perma.cc/7757-5D2T].

[213] *See Adequacy Decisions*, *supra* note 107. As of the writing of this Paper, Brazil and the EU are in negotiations concerning an adequacy decision. *International: Brazil and EU Work to Finalize Mutual Adequacy Decision*, ONETRUST DATA GUIDANCE (Mar. 22, 2024), https://www.dataguidance.com/news/international-brazil-and-eu-work-finalize-mutual [https://perma.cc/WS6N-HUEX].

[214] To the extent that the country where ACME Cyber Sentinel is headquartered has data protection and/or AI regulations that impact this assessment, these requirements are beyond the scope of this Paper.

[215] *Schrems II*, Case C-311/18. To date, enforcement actions have been primarily limited to actions involving transfers to U.S.-based companies. *See* Hiscock, *supra* note 211.

[216] *Schrems II*, Case C-311/18 ¶¶ 126, 133, 135; CHRISTAKIS, *supra* note 124.

authorities of third countries."[217] *Schrems II* instructs controllers to "suspend or end the transfer of personal data to the third country concerned" when they cannot guarantee that a processor is ensuring an appropriate level of protection.[218]

The actions taken by various DPAs during the time between the CJEU's invalidation of the Privacy Shield in the 2020 *Schrems II* case and the official implementation of the Data Privacy Framework in 2023 provide a cautionary tale both for U.S.-based companies, if the current adequacy decision was to be invalidated, as well as for companies based in third countries.[219] European

---

[217] *Schrems II*, Case C-311/18 ¶132.

[218] *Id.* ¶ 135.

[219] In 2021, the Portuguese Data Protection Authority (Comissão Nacional de Proteção de Dados, the "CNPD") found that the use of Cloudflare, a service provider headquartered in the United States, by Portugal's National Institute of Statistics ("INE") to process data for Portugal's 2021 national census did not meet the requirements of EU data protection law. *CNPD Portugal – Deliberação 2021/533*, GDPRHUB (2021), https://gdprhub.eu/index.php?title=CNPD_(Portugal)_-_Delibera%C3%A7%C3%A3o_2021/533 [https://perma.cc/C47N-V8QT]. The CNPD ordered INE to "suspend the sending of personal data" concerning the census to the United States. *Id.*; *see Portuguese DPA Orders Suspension of U.S. Data Transfers by Agency That Relied on SCCs*, HUNTON ANDREWS KURTH (Apr. 28, 2021), https://www.huntonak.com/privacy-and-information-security-law/portuguese-dpa-orders-suspension-of-u-s-data-transfers-by-agency-that-relied-on-sccs [https://perma.cc/HWJ6-5KHK]. The CNPD based its reasoning on the *Schrems II* decision, finding that INE could not ensure that EU personal data transferred to the United States was afforded a level of data protection that was essentially equivalent to the guarantees under EU law. *Id.* Citing to the *Schrems II,* the CNPD found that INE was obliged to suspend these data transfers, even when those transfers were based on SCCs. *Id.* This decision by the CNPD ultimately required INE to stop using a cybersecurity service meant to defend against cyber threats. Keir Lamont & Alex Roure, *Portuguese Decision Another Foreboding Sign for Global Data Transfers*, DISCO (May 7, 2021), https://project-disco.org/european-union/050721-portuguese-decision-another-foreboding-sign-for-global-data-transfers/ [https://perma.cc/D6MA-LLZL]; *CNPD Portugal – Deliberação 2021/533*, *supra* note 219; *see also* Peter Swire & DeBrae Kennedy-Mayo, *New Urgency About Data Localization with Portuguese Decision*, IAPP (Apr. 29, 2021), https://iapp.org/news/a/new-urgency-about-data-localization-with-portuguese-decision/ [https://perma.cc/WPX6-PGSR]. Also in 2021, the Data Protection Authority of the German State of Bavaria (Bavarian DPA), determined that the sharing of email addresses with Mailchimp, an email marketing platform headquartered in the United States, by an unnamed German company (for the purpose of sending newsletters to the company's own customers) constituted an unlawful transfer. *Bavarian DPA (BayLDA) Calls for German Company to Cease the Use of Mailchip Tool*, EDPB (Mar. 30, 2021), https://www.edpb.europa.eu/news/national-news/2021/bavarian-dpa-baylda-calls-german-company-cease-use-mailchimp-tool_en [https://perma.cc/59A9-DQ4V]. Grounding its decision in the reasoning in *Schrems II,* the Bavarian DPA concluded that there were "at least indications that Mailchimp may in principle be subject to data access by U.S. intelligence services." Keir Lamont, *The Monkey's Pause: Mailchimp Data Transfers Halted in German Schrems II Inquiry*, DISCO (Apr. 6, 2021), https://project-disco.org/

scholar Théodore Christakis observed that numerous European DPAs implemented a "zero-risk" approach since the *Schrems II* case, where data controllers are expected to eliminate all risks of access to EU personal data by governments of third countries.[220] According to Christakis, the strictest interpretation of the "zero-risk" approach appears to consider access to personal data by a company based in a third country to be prohibited under EU data protection law—even if that data remains in the EU.[221]

Assuming that ACME Cyber Sentinel is based in a country without an adequacy decision, the company's SCCs (or even its BCRs) must be accompanied by "supplementary measures" to provide a "contractual guarantee of an adequate level of protection against access by the public authorities of that third country to that data."[222] For this scenario where TechGuard is acting as the controller and ACME Cyber Sentinel is likely in the role of a processor, there is a potential for a DPA in the EU to apply the requirements of *Schrems II* in such a way that could force TechGuard to suspend transfers of personal data to ACME Cyber Sentinel, particularly when this company is envisioned to have its headquarters in a third country that lacks an adequacy decision.

For Scenario 1, the lawfulness of ACME Cyber Sentinel providing services within the EU turns on facts of what is personal data and sensitive personal data, and whether a lawful basis exists for such processing.[223] When ACME Cyber Sentinel is based outside the EU in a country without an adequacy decision, the legal requirements for the company are significantly more complex.

B. Analysis for Scenario 2

Scenario 2 focuses on ACME Cyber Sentinel gathering a limited amount of data from ten clients, including TechGuard, to help identify and respond to new cybersecurity threats. This means that the purpose of gathering the data is to improve cybersecurity services. The questions for this scenario are: Is the data stored and analyzed by ACME Cyber Sentinel considered personal data? Is ACME Cyber Sentinel a joint controller of the data collected from the ten companies? What is the lawful basis for ACME Cyber Sentinel to

---

european-union/040621-the-monkeys-pause-mailchimp-data-transfers-halted-in-ger man-schrems-ii-inquiry/ [https://perma.cc/687R-BQ4V]. The Bavarian DPA instructed the unnamed German company to immediately cease using the services of Mailchimp. *Id.*; *see Bavarian DPA (BayLDA) Calls for German Company to Cease the Use of Mailchip Tool*, *supra* note 219.

[220] Christakis analyzed enforcement actions involving U.S.-based companies. CHRISTAKIS, *supra* note 124; *see Techniques, Tactics, and Procedures*, *supra* note 5, at 11.

[221] Under this interpretation, the risk that the government in the third country can access the EU personal data must be eliminated. CHRISTAKIS, *supra* note 124, § 2.1.

[222] *Schrems II*, Case C-311/18 ¶¶ 126, 133, 135; CHRISTAKIS, *supra* note 124.

[223] Our research has not found authoritative legal pronouncements on these precise issues, including from the CJEU or the EDPB.

process this data? Can the personal data be transferred to ACME Cyber Sentinel?

1. Is the data stored and analyzed by ACME Cyber Sentinel considered personal data?

The initial question that needs to be answered in this scenario relates to whether the data that ACME Cyber Sentinel gathered from the ten companies constitutes personal data.[224] As a reminder, if the data does not constitute personal data, then the GDPR will not apply.[225]

Data that explicitly mentions a natural person is unlikely to be categorized as anything other than personal data. Therefore, if ACME Cyber Sentinel is given, for example, a database of users by TechGuard, ACME Cyber Sentinel should likely assume that the GDPR rules for personal data will apply.

Conversely, data that is unrelated to a natural person is likely to fall outside of the GDPR's scope because the definition of personal data states that the data must relate to an identified or identifiable natural person.[226] Later in this analysis, the Article will return to the situation of what appears to be non-personal data, where there is the possibility of subsequently linking the data to a natural person.

Data derived from a natural person's activity is more nuanced than information generated by, and related to, the activities of a natural person. For example, the case of *Digital Rights Ireland* addressed to some degree whether log files and associated meta data can constitute personal data,[227] which was answered in the affirmative. Because this case predates the GDPR and was heard under the auspices of the Data Protection Directive (the pre-cursor to the GDPR),[228] a question exists as to whether this position was clarified by the GDPR. The answer can only be described as "yes, but insufficiently." The crux of the question turns on whether log data, which does not in and of

---

[224] As a reminder, the categories of data relevant in this scenario include: data that explicitly mentions a natural person (e.g., a database of users); data that is derived from the activity of a natural person (e.g., log files which relate to a user's activity or which contain references to users); data that is unrelated to a natural person (e.g., an application log file which does not contain any user data); and data that contains information which could be used to identify a natural person, given some other information which is not held by TechGuard (e.g., a list of IP addresses which accessed TechGuard's resource).

[225] GDPR, *supra* note 1, art. 1(1).

[226] *Id.* art. 4(1).

[227] Joined Cases C-293/12 & C-594/12, Digit. Rts. Ireland Ltd. v. Minister for Commc'ns Marine and Nat. Res., 2014, ¶ 17–18, High Court, Ireland, Apr. 8, 2014 (examining, *inter alia*, whether the retention of meta data and log data from telephone providers was processing of personal data).

[228] Directive 95/46/EC On The Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data, O.J. (L 281), 23/11/1995 P. 0031-0050 (1995).

itself contain explicit personal data (such as the user's name or email address), can be considered personal data.

One challenge for ACME Cyber Sentinel is whether this seemingly non-personal data, which has been collected from the ten companies, is viewed—from a legal perspective—as transformed into personal data. As discussed in Scenario 1, the CJEU in *Breyer* and *Nowak* concluded that IP addresses, which by themselves do not constitute personal data under EU law, are considered *de facto* elements of personal data if, under any circumstances, there exists a legal right for the processor to compel the release of the personal data.[229] Regarding ACME Cyber Sentinel, it is likely that if data at issue has been provided to the company to assess whether an individual poses a threat to the cybersecurity of the network, then some or all of the dataset may be considered as personal data. This conclusion likely holds even if this dataset's constituent elements do not contain personal data, given that this data profiles individual behavior and identifies the threat and risk associated with a natural person.

Another challenge for ACME Cyber Sentinel is whether these log files, which may be "pseudonymous" data, constitute personal data. Pseudonymous data has been amended so it can no longer be attributed to an individual without the provision of additional information.[230] An example would be a log file which contains a user ID, as the processor would need to possess, or have access to, the table that links a user ID to the identity of the user. European academics Fink and Pallas provide an excellent history of how the CJEU and the EDPB have differing views regarding whether pseudonymous data constitutes personal data. These academics note how the EDPB has taken an absolute position that pseudonymous data will always constitute personal data if there remains any way for the controller to reidentify the data subject. The academic authors point out, in contrast, that the Recitals in the GDPR and certain decisions by the CJEU suggest the use of a risk-based approach to determine, on a case-by-case basis, whether pseudonymous data is personal data.[231]

The question of approach is highly relevant to ACME Cyber Sentinel, as the answer will determine whether information obtained from TechGuard is subject to the GDPR. This is because anonymous data (data whereby it is not possible to determine the identity of the underlying user)[232] is not subject to the GDPR, while pseudonymous data, under the EDPB guidance, will always

---

[229] Patrick Breyer v. Bundesrepublik Deutschland, Case C-582/14, ¶ 49, Bundesgerichtshof [BGH] [Federal Court of Justice] Oct. 19, 2016; Nowak v. Data Protection Comm'r, Case C-434/16, ¶¶ 31, 33, Supreme Court (Ireland), Dec. 20, 2017. Although the outcomes in the two cases are similar, the facts of *Breyer* and *Nowak* differ.

[230] GDPR, *supra* note 1, art. 4(5).

[231] Michèle Finck & Frank Pallas, *They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data under the GDPR*, 10 INT. DATA PRIV. LAW 11 (2020).

[232] GDPR, *supra* note 1, at 5.

be personal data, even if ACME Cyber Sentinel is unable to identify the data subject.[233]

The alternative, less absolutist, approach to differentiating between anonymous and pseudonymous data is a risk-based approach,[234] whereby the data is deemed anonymous (and hence no longer personal data) when the risk of re-identification falls to an acceptable minimal level.[235] Although the GDPR does not stipulate what this acceptable minimal level is, Recital 26 to the GDPR suggests that, when assessing whether data has been anonymized or merely pseudonymized, the data protection regulator or the court will look at all "the means reasonably likely to be used . . . , either by the controller or by another person to identify the natural person directly or indirectly."[236] The Recital also provides guidance as to what activities constitute "reasonable means" when assessing "whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments."[237] Although not formally enshrined within the text of a GDPR article, the GDPR suggests anonymity does not need to be absolute in order for data to be deemed non-personal data. This contradicts the approach outlined by the EDPB and suggests that it may be possible for a business that has followed sufficient anonymization processes to provide

---

[233] *Id.* at 13–15. The Article 29 Working Party, the forerunner to the EDPB, released guidelines in 2014 with regards to anonymization and pseudonymisation of data. These guidelines can be said to hold an absolute position with regards to the topic. ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 05/2014 on Anonymisation Techniques* (Apr. 10, 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf [https://perma.cc/QK2S-BHET]. Under their guidelines, it was proposed that unless the data controller first engages in a process to remove personal identifiers from the data (anonymisation), and then deletes the original data, the 'anonymous' data will still be considered as personal data. *Id.* at 9; *see also* EDPB, *Legacy: Art. 29 Working Party*, https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_en [https://perma.cc/CAS8-YAWT] (last visited June 13, 2024). Under this regime, it would never be possible, on a practical basis, for a business to ever give ACME Cyber Sentinel non-personal data, so long as the business retained the original personal data and the result would be that ACME Cyber Sentinel is likely to be deemed a controller with regard to any processing that it undertakes on any explicit personal data or psuedonomous information given by the business. *See* GDPR, *supra* note 1.

[234] *See, e.g.*, Emily M Weitzenboeck et al., *The GDPR and Unstructured Data: Is Anonymization Possible?*, 12 INT. DATA PRIV. LAW 184, 191 (2022) (analyzing a more in-depth discussion of the risk based approached).

[235] *Id.* It must be noted how these approaches can also be known as the "subjective" (risk based) and "objective" (strict) approach. *See, e.g.*, Lore Leitner et al., *Anonymisation Through Separation: What Recent Cases Teach Us about the EU's Anonymisation Standards*, 24 PRIV. DATA PROT. 10, 11 (2024).

[236] GDPR, *supra* note 1, at 5; *see* Weitzenboeck, *supra* note 235. It must be noted how Recitals are illustrative, as opposed to authoritative text.

[237] GDPR, *supra* note 1, at 5.

anonymous data to ACME Cyber Sentinel and thus remain outside of the scope of the GDPR without having to erase the personal elements of the information in question from its own data storage.

Breyer was the first time the CJEU ruled on what constituted personal data following an anonymization process. In this ruling, the CJEU invoked Recital 26,[238] given the judgment focused on the question of whether the recipient of the IP address (the website) could de-anonymize it.[239] The CJEU took the view that the test for anonymization is from the recipient's perspective, and not on whether merely any party involved in processing the data could establish the details of the data subject.[240]

This question was revisited in the 2023 case of *Single Resolution Board* ("SRB") *v. European Data Protection Supervisor* ("EDPS"), where the CJEU examined the extent that pseudonymization can convert personal data to non-personal data from the perspective of third parties who the data was shared with.[241] This case relates to an appeal against a finding by the EDPS that the SRB had breached the GDPR by transferring "personal data" insufficiently anonymized to Deloitte without informing the data subjects of Deloitte's involvement.[242] The court's judgment appeared to explicitly rule out the approach taken first by the Article 29 Working Party and later by the EDPS.[243] Under that approach, the fact that the SRB continued to hold the personal data in question was sufficient to determine that Deloitte was provided with

---

[238] Patrick Breyer v. Bundesrepublik Deutschland, Case C-582/14, ¶¶ 3, 42, Bundesgerichtshof [BGH] [Federal Court of Justice] Oct. 19, 2016.

[239] *Id.* ¶ 49. It is noteworthy that the court answered the question as to whether the IP address constituted personal data from the perspective of the website host, and not from the ISP. *Id.* ¶ 31. While in this case, the IP address was held to be personal data, this was only due to the fact that the website did have a potential lawful means to compel the ISP to disclose the identity of the user associated with the IP address. *Id.* ¶¶ 24, 49. If this potential compulsion was not possible, it is clear that the data would not have been found to be personal data, even though the ISP (the data controller) would have been able to identify the data subject. *Id.*

[240] Although this would suggest that the court has rejected the Article 29 Working Party's guidelines with regards to anonymization and pseudonymization, it is important to note that *Breyer* did not refer to the Article 29 Working Party's guidelines and was silent on the approach as outlined by the EDPB. See D. Groos & E. Van Veen, *Anonymised Data and the Rule of Law*, 6 EUR. DATA PROT. L. REV. 498 (2020), for a similar argument.

[241] Single Resolution Board (SRB) v. European Data Protection Supervisor (EDPS), Case T-557/20, ¶ 79, Apr. 26, 2023.

[242] *SRB*, Case T-557/20 ¶¶ 2–32. The European Data Protection Supervisor is the Data Protection Regulator for the processing of personal data which is carried out by European Union Institutions. For more information on the EDPS, see *Data Protection,* EDPS, https://www.edps.europa.eu/data-protection_en [https://perma.cc/AE9M-LLCD] (last visited June 12, 2024).

[243] The Article 29 Working Party is the forerunner to the EDPB. *Legacy: Art. 29 Working Party*, EDPB, https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_en [https://perma.cc/WEX4-8UAP] (last visited Aug. 23, 2024).

personal data.[244] The CJEU stated, however, that there were two relevant questions for the EDPS to consider: (1) whether, in fact, Deloitte had a legal means to combine the data held by the SRB with its provided data; and (2) whether it was reasonable to assume that Deloitte was likely to use this additional (but not received) information to identify the data subjects.[245] While it must be acknowledged that this decision has been appealed by the EDPS,[246] and therefore this interpretation is subject to change, the decision in *SRB v. EDPS* suggests that a controller can pseudonymize data and distribute it to third parties where it will be deemed to be outside of the scope of the GDPR, so long as it is reasonable to assume that the third party will not be able to re-identify the underlying data subjects.

It is important to remember from *Breyer* that the mere existence of a single legal basis in which the third party can, even under remote and unlikely circumstances, compel disclosure of the identity of the data subjects is enough to rebut the presumption of anonymization.[247] In the context of ACME Cyber Sentinel and TechGuard, in order for the presumption of anonymization to hold, they must ensure that their contractual relationships do not give rise to the ability for ACME Cyber Sentinel to seek the personal information of the data subject.

Assuming that the appellate court does not reverse the *SRB v. EDPS* decision, it appears that a data controller such as TechGuard retains the possibility of providing suitably pseudonymized data to a third party such as ACME Cyber Sentinel for processing.

The *Scania* case,[248] however, provides a warning to both ACME Cyber Sentinel and TechGuard with regard to the processing of anonymous data. In this case, the court questioned whether Vehicle Identification Numbers ("VINs") were personal data when made available to people (mechanics and truck repair companies) who were reasonably able to link the VINs to specific natural persons.[249] Ultimately, the court deemed the VINs as non-personal data, as they related to vehicles and not natural persons. In the case, Scania made information relating to vehicles available to third-party mechanics and vehicle repair companies, and this information could be obtained by querying a specific VIN.[250] But, given the fact that the VIN was known to be on the vehicle licensing certificate, which contained personal data relating to the

---

[244] *SRB*, Case T-557/20 ¶¶ 97–106.

[245] *Id.* ¶¶ 105–06.

[246] EDPS v. SRB, Case C-413/23 P, Svea hovrätt, Patent- och marknadsöverdomstolen [Sweden] June 15, 2023.

[247] It has been noted by some practitioners that this was a missed opportunity for the CJEU to formally rebut the approach taken in the Art 29 Working Party guidance. *See* Ali Vaziri, *Pseudonymous or Anonymous, That Is the Question*, 23 PRIV. DATA PROT. 10, 12 (2023).

[248] Gesamtverband Autoteile-Handel v. Scania, Case C-319/22, Landgericht Köln [Regional Court, Cologne, Germany] Nov. 9, 2023.

[249] *Id.* ¶ 46.

[250] *Id.* ¶ 36.

registered owner or user of the vehicle, and given how it was reasonable that some mechanics and servicing personnel who were able to access the VIN from the controller, were also likely to have access to the licensing certificate, the VIN was considered personal data.[251] Consequently, Scania was deemed to be a controller of personal data when processing VINs.[252] This demonstrated that when an entity enables the processing of information, which it does not consider personal data, by a subset of third parties with independently obtained information from the first party and can derive the identity of the data subject, both parties will be processing personal data.

Applying *Scania* to TechGuard and ACME Cyber Sentinel, it is likely that at least some cybersecurity companies have access to the data, which would remove the presumption of anonymity for data transferred between TechGuard and ACME Cyber Sentinel. One potential analogue could be data extracted by criminals during a cyber-breach, especially where the data becomes public on the internet. Where such a posting includes data that ACME Cyber Sentinel could use to re-identify the data subjects, then this data is likely to be viewed as personal data irrespective of the pseudonymization transformation carried out by TechGuard. As such, when evaluating data made available to ACME Cyber Sentinel by TechGuard, it would be prudent for ACME Cyber Sentinel to ensure that no "related" information is known to have been extracted from TechGuard by a cyberattacker. Additionally, ACME Cyber Sentinel should verify that it is not aware of any information that has been obtained from other sources, which can be used to identify the data subjects in pseudonymized data. The prudent approach would be to receive this information on a pseudonymized basis only if ACME Cyber Sentinel was comfortable that additional information was not made available from third parties, enabling the re-identification of data subjects.

If ACME Cyber Sentinel has any potential means to re-identify the data subjects, then, according to *Breyer*, *SRB*, and *Nowak*, it seems likely that the CJEU will deem the data to be personal data even if ACME Cyber Sentinel has not actually used these means.

2. Is ACME Cyber Sentinel a controller of the data collected from the ten companies?

This subpart begins by returning briefly to Scenario 1. In the relationship between ACME Cyber Sentinel and one client, TechGuard, it may be a situation where TechGuard has provided ACME Cyber Sentinel with specific instructions relating to the update of the cybersecurity services for TechGuard's benefit by utilizing pertinent personal data from TechGuard's clients and employees.[253] Under these facts, ACME Cyber Sentinel would

---

[251] *Id.* ¶ 46–47.

[252] *Id.* ¶ 62.

[253] *See Subcontractors: The Reuse of Data Entrusted by a Data Controller*, CNIL (Jan. 11, 2022) (translated from French), https://www.cnil.fr/fr/sous-traitants-la-reutilisation-de-donnees-confiees-par-un-responsable-de-traitement [https://perma.

likely be acting as a processor.[254] Scenario 2 becomes more complicated when the personal data of all ten companies are combined for the purpose of updating the tools of ACME Cyber Sentinel.

When AMCE Cyber Sentinel processes the personal data from ten companies to identify and respond to new cybersecurity threats, it is more likely to be a controller.[255] ACME Cyber Sentinel collects personal data from TechGuard, and then performs a series of processing activities upon this personal data, including processing this personal data directly with other personal data sourced from other businesses. In an effort to improve its cybersecurity services, ACME Cyber Sentinel stores and analyzes limited amounts of information gathered from each client, considered potential new cyber threats. This data, collected from Businesses 1 to 10, is then consolidated with other datasets held by ACME Cyber Sentinel. ACME Cyber Sentinel then responds to particular cybersecurity threats identified at each of the ten companies. These activities demonstrate that ACME Cyber Sentinel, and only ACME Cyber Sentinel, determines the exact form of processing that will take place on the personal data collected from Businesses 1 to 10 and how this personal data will interact with ACME Cyber Sentinel's other personal data collected from the other businesses.

When examining the role of the ACME Cyber Sentinel in this scenario, the key inquiries are whether this company controls the why (purpose) and

---

cc/DSZ7-PETS]; *see also* Anne-Gabrielle Haie & Loraine Sangaré-Vayssac, *France Issues Processor Guidelines on "Reusing Personal Data to Improve or Develop Services or Products"*, COOLEY (Feb. 9, 2022), https://cdp.cooley.com/france-issues-processor-guidelines-on-reusing-personal-data-to-improve-or-develop-services-or-products/ [https://perma.cc/BY8M-4RCY].

[254] The EDPB states that "mutual benefit" is not sufficient to establish joint controllership unless both entities are involved in the "determination of the purposes and means of the relevant processing operation." *Guidelines on the Concepts of Controller and Processor*, *supra* note 57, ¶ 60. In an example involving the analysis of health data, the EDPB finds that the company being asked to perform an assessment acts as a processor when it has no purpose of its own, even though the company "may benefit from the assessment by using its results in their own activities." *Id.* ¶ 68. This line between processor and joint controller can be envisioned as a fairly narrow one, as the CJEU held that a website operator and a provider of a plug-in on a website were joint controllers in part because the processing was performed in the economic interests of each party. Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV, Case C-40/17, ¶ 80 [Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany)] July 29, 2019; *see Guidelines on the Concepts of Controller and Processor*, *supra* note 57, ¶ 60.

[255] This assessment assumes that ACME Cyber Sentinel is processing personal data when it accesses this data, as discussed in Section IV.B.1. It is worth noting that the EDPB also includes an example of a company providing IT services to fix a "software bug." The EDPB explained that, where access to personal data is very limited and would be incidental to the service provided, the IT company is deemed to be neither a processor nor a controller. *Guidelines on the Concepts of Controller and Processor*, *supra* note 57, ¶ 83.

the how (means) of processing this data for cybersecurity purposes.[256] When TechGuard determines that the data will be processed for the purposes of providing cybersecurity services in Scenario 1, is it reasonable to say that the ACME Cyber Sentinel meets the definition of a controller because it has determined the purpose for the processing of the data when it seeks to improve its cybersecurity services?

A controller simply "determines the purposes and means of the processing of personal data."[257] As discussed in Scenario 1 regarding the means of processing, the EDPB identifies a distinction between "essential means" and "non-essential" means of processing.[258] Important to the discussion of ACME Cyber Sentinel's processing to improve cybersecurity services, essential means are reserved only for controllers because these means are closely associated with the purpose and scope of the processing—"the type of personal data which are processed ('*which data shall be processed?*'), the duration of the processing ('f*or how long shall they be processed?*'), the categories of recipients ('*who shall have access to them?*') and the categories of data subjects ('*whose personal data shall be processed?*')."[259] Depending on the facts, ACME Cyber Sentinel may make judgments, based on its professional expertise, on each of these "essential means" inquiries regarding the personal data gathered by ACME Cyber Sentinel from TechGuard or the other businesses (irrespective the businesses that the data was collected from)—such as to establish the cybersecurity risk associated with a particular element. If so, then ACME Cyber Sentinel will likely be viewed as a controller, not a processor, for the processing activity at issue in this scenario.

When examining the controller question for the processing related to improving cybersecurity services, the EDPB's example of the telecom operator is particularly instructive—with one variation where the telecom operator is a processor and another where it is a controller. The telecom operator acts as a processor when providing the service of transmitting emails, meaning it is *not* considered the controller of the content of the email messages (assuming the only processing that the telecom operator undertakes related to the emails is transmission). This provider of an electronic communication service is typically the controller where the "processing of personal data . . . is necessary for the operation of the service," such as processing traffic data and billing data.[260] As discussed in detail in Scenario 1, ACME Cyber Sentinel likely acts as a processor when accessing the personal data of TechGuard for the purpose of providing cybersecurity

---

[256] *Guidelines on Consent*, *supra* note 55, art. 2.1.4; *see id.* ¶ 33.

[257] GDPR, *supra* note 1, art. 4(7); *see Guidelines on the Concepts of Controller and Processor*, *supra* note 57, ¶ 20 (stating that a controller makes "an exercise of decision-making power" that focuses on control over the processing of the personal data).

[258] *Guidelines on the Concepts of Controller and Processor*, *supra* note 57, ¶ 40.

[259] *Id.*

[260] *Id.* ¶ 27.

services. When ACME Cyber Sentinel is processing telemetry from Businesses 1 to 10 to *improve* its cybersecurity services, however, this activity is related to the operation of its cybersecurity service, meaning that ACME Cyber Sentinel is likely acting as a controller when processing personal data for this purpose.

Assuming that ACME Cyber Sentinel is viewed as a controller of the personal data being processed for the purpose of improving cybersecurity services, a next issue is whether it will be a joint controller with TechGuard, or an independent controller. As with the analysis of processor or controller, this inquiry will depend on the facts.[261] Here, we provide two variations. In the first set of facts, ACME Cyber Sentinel is a joint controller with regard to the personal data at issue in Scenario 2. In the second set of facts, ACME Cyber Sentinel acts as an independent, separate controller. Being designated a joint controller means that both companies are responsible, on a joint and several basis,[262] for the processing of the data subjects' personal data.[263]

In the first variation of Scenario 2, the contract between ACME Cyber Sentinel and a client includes language that says that ACME Cyber Sentinel will collect and analyze information, relevant to potential new cyber threats, to assist ACME Cyber Sentinel's clients in the future.[264] This variation may result in joint controllership for ACME Cyber Sentinel.

Joint controllership exists where each entity takes part in determining the purposes and means of the particular processing.[265] *Facebook Fanpage* is the leading relevant case from the CJEU in determining joint controllership.[266] In this case, statistics related to individuals who visited the fanpage were used by Facebook to improve its advertising services, while the administrator of the fan page used these statistics to assist with promoting its activities.[267] Both Facebook and the administrator of the fanpage were deemed to be joint controllers.[268] The joint controller status applied, however, only with regard to the processing activities which were common to them both (the population statistics).[269]

---

[261] *See id.* ¶ 52.

[262] GDPR, *supra* note 1, art. 26(3).

[263] *Id.* art. 26.

[264] For purposes of the scenario, we assume the language in contract mirrors the actual relationship between the parties.

[265] *Guidelines on the Concepts of Controller and Processor*, *supra* note 57, ¶ 53; *see id.* ¶ 58 ("The existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data.").

[266] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH, Case C-210/16, Bundesverwaltungsgericht [Federal Administrative Court, Germany] June 5, 2018 (*Facebook Fanpage Case*).

[267] *Id.; see Guidelines on the Concepts of Controller and Processor*, *supra* note 57, ¶¶ 61, 65.

[268] *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, Case C-210/16 ¶ 44.

[269] *Id.* ¶ 43.

Joint participation can also be achieved by converging decisions. The EDPB finds converging decisions when "the processing would not be possible without both parties' participation in the purposes and means in the sense that the processing by each party is inseparable, i.e., inextricably linked."[270] This concept has been discussed by the CJEU in the *Jehovah's Witnesses* case,[271] where it was noted that religious organization's members that engage in door-to-door preaching are considered joint controllers even when the organization does not have access to the personal data being processed by the door-to-door preachers, or has not provided the preachers with written guidelines or instructions.[272]

The EDPB explores the concept of converging decisions in its example of a headhunting firm and its client company. The headhunting firm manages a database of resumes from companies it has previously interacted with and offers a service for finding suitable candidates for employment by its clients. The client company "enrich[es] the database" of the headhunting firm with resumes that the client has received directly.[273] This activity by the client company allows the headhunting firm to assist the client company in recruiting new employees; the headhunting firm benefits by having more resumes to match. Because these "decisions complement each other, are inseparable and necessary for the processing of finding suitable candidates," the headhunting firm and the client company are joint controllers engaged in converging decisions for this processing.[274]

ACME Cyber Sentinel may similarly become a joint controller when it maintains a database of new cyber threats and adds potential new threats from Businesses 1 to 10. Like the headhunting firm, ACME Cyber Sentinel may "enrich the database" to improve cybersecurity services via the detection of new cyber threats. The scope of any such joint controller status is limited—TechGuard's role as controller is most likely limited to only the processing of the personal data that ACME Cyber Sentinel collected from TechGuard.

In the second variation of Scenario 2, the contract between ACME Cyber Sentinel and each of its clients is silent as to the processing related to ACME Cyber Sentinel improving its cybersecurity services. ACME Cyber Sentinel determines the purpose for this processing (to improve its cybersecurity services) and the means (by collecting and analyzing limited amounts of information from each client to determine whether such data represents a new cyber threat and by adding any data determined to be a cyber threat to its database). Under this variation, ACME Cyber Sentinel likely acts as an independent controller for the personal data to improve its cybersecurity services. The EDPB guidance provides a flowchart and states that the key to determining whether an entity acts as an independent controller for a

---

[270] *Id.* ¶ 55.

[271] Tietosuojavaltuutettu v. Jehovan todistajat, Case C-25/17, Korkein hallinto-oikeus [Supreme Administrative Court, Finland] July 10, 2023.

[272] *Id.* ¶ 75.

[273] *Guidelines on the Concepts of Controller and Processor*, *supra* note 57, ¶ 68.

[274] *Id.* ¶ 68.

particular processing activity is that the entity "decides alone the purposes and means" for the processing activity.[275]

Another EDPB example, concerning a travel agency, explores the distinctions between joint controllers and separate controllers. When three entities—the travel agency, the airline, and the hotel—work together to offer travel package deals on a common online platform, then they are joint controllers. By contrast, when each entity carries out its own activities, without a common online platform, they may be separate controllers.[276] ACME Cyber Sentinel's role in updating its cybersecurity services can be seen to be analogous to the travel agency when it is acting as a separate controller, with ACME Cyber Sentinel using certain personal data from the other two companies to achieve its purpose (updating its cybersecurity services).

In sum, ACME Cyber Sentinel and the other businesses likely act as joint controllers when these businesses are aware of and participate in the purpose and the means of processing for updating ACME Cyber Sentinel's cybersecurity services. Conversely, ACME Cyber Sentinel likely acts as a separate controller without joint participation in the purpose and the means of processing. The examples provided by the EDPB suggest that ACME Cyber Sentinel probably acts as a separate controller for purposes of maintaining its database of new cyber threats.

3. What is the lawful basis for ACME Cyber Sentinel to process this data?

In examining the lawfulness of processing data, a contract cannot give *carte blanche* to TechGuard or ACME Cyber Sentinel to implement cybersecurity practices that require processing substantial amounts of personal data. The limits on the contract as a legal basis have been explored in the binding *Meta Platforms* decision by the EDPB, which examined, *inter alia*, whether Meta could include the processing of personal data for behavioral-based advertisement targeting as necessary for the performance of

---

[275] *See id.* at 51. If one of these entities decides alone the purposes and means of operations that precede or are subsequent in the chain of processing, this entity must be considered as the sole controller of this preceding or subsequent operation." *Id.* ¶ 57 (citing Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV, Case C-40/17, ¶ 74 [Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany)] July 29, 2019); *Fashion ID*, Case C-40/17, ¶ 74 ("By contrast, and without prejudice to any civil liability provided for in national law in this respect, that natural or legal person cannot be considered to be a controller, within the meaning of that provision, in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means.").

[276] *Guidelines on the Concepts of Controller and Processor*, *supra* note 57, ¶ 68.

a contract.[277] The original decision by the Irish Data Protection Commissioner held that, while processing personal data for behavioral advertisement purposes would not normally constitute a valid example of processing necessary for the performance of a contract, in this case, and given the specifics of the Meta Terms of Service, it did.[278] Other European Data Protection Regulators,[279] however, argued that this would create a loophole for controllers to make lawful almost any processing of personal data so long as it was deemed necessary for the performance of a contract.[280] The EDPB decision commented that Article 6(1)(b) of the GDPR "does not cover processing which is useful but not objectively necessary for performing the contractual service, even if it is necessary for the controller's other business purposes."[281]

Furthermore, the EDPB states that an additional requirement for the valid use of Article 6(1)(b) of the GDPR is that the data subject must be provided with sufficient information to understand how the processing of personal data is necessary for the performance of the contract.[282] For ACME Cyber Sentinel to rely on Article 6(1)(b) of the GPDR, the provision of its service must be, on an objective basis, necessary in order for the contract to be performed.

The most likely approach for ACME Cyber Sentinel to ensure a lawful basis for processing personal data is that of "legitimate interests," based on the legitimate interests of either the controller or a third party.[283] This ground for processing is not available to public authorities, raising a question of how such authorities would gain access to cybersecurity services.[284]

In *Rigas Satiksme*,[285] the CJEU discussed the limits on this basis for processing. *Rigas Satiksme* set forth a three-part test that must be satisfied for an entity to claim a legitimate interest as a lawful means of processing: (1) the processing is carried out in the pursuit of the legitimate interest of the controller or a third party; (2) there is a need to process the personal data in

---

[277] *Binding Decision 3/2022 on the Dispute Submitted by the Irish SA on Meta Platforms Ireland Limited and Its Facebook Service (Art. 65 GDPR)*, EDPB (Dec. 5, 2022), https://www.edpb.europa.eu/system/files/2023-01/edpb_bindingdecision_202203_ie_sa_meta_facebookservice_redacted_en.pdf [https://perma.cc/NNP7-XCCK].

[278] *Id.* ¶ 114.

[279] The Austrian, German, French, Italian, Dutch, Norwegian, Polish, Portuguese and Swedish regulators disagreed with the decision of the Irish DPC. *Id.* ¶ 81.

[280] *Id.* ¶ 61.

[281] *Id.* ¶ 121.

[282] *Id.* ¶ 126.

[283] GDPR, *supra* note 1, art. 6(1)(f).

[284] *Id.* art. 6(1).

[285] Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA 'Rīgas satiksme,' Case C-13/16, Augstākās tiesas, Administratīvo lietu departaments [Supreme Court, Administrative Division, Latvia] May 4, 2017.

pursuit of the legitimate interest; and (3) the consequence of processing is weighed against the fundamental rights of the data subject(s) in question.[286]

In the subsequent case of *Meta Platforms v. Bundeskartellamt*, however, the CJEU touched on the use of legitimate basis for processing personal data for cybersecurity purposes, and confirmed that the processing of data for the purposes of ensuring network security is a legitimate interest of the controller.[287] When legitimate interests basis is used, the reviewing authority must determine whether the processing activities were actually necessary to maintain the security of the controller's networks.[288] The CJEU noted it was impossible to make such a determination in the case based on the information provided.[289] There is no indication yet from the CJEU as to what latitude it is willing to provide to controllers with regard to cybersecurity data processing. The CJEU also confirmed that when this basis is used for the processing of personal data, the data subject must be informed of the legitimate interest,[290] and they must sustain reasonable expectations that their data will be processed by the controller for this legitimate interest.[291]

While Article 6(1)(f) appears to provide a means for the controller to process the data subject's collected personal data, both ACME Cyber Sentinel and TechGuard will need to demonstrate to a supervisory authority that this form of data processing was required, that the user was informed of the reason for the processing,[292] and that the *Rigas Satiksme* balancing test was carried out and answered in the affirmative. For special categories of data, there is no lawful basis of processing which is equivalent to legitimate interests.[293]

Legitimate interests are also a basis for information sharing between cybersecurity companies. Author Andy Greenberg explains how iSight, a cybersecurity company that had identified malware used to infiltrate and destabilize Ukrainian critical infrastructure in 2017, made details of the malware publicly available, including potential personal data such as IP

---

[286] *Id.* ¶ 28. The *Rigas Satiksme* case was heard under the Data Protection Directive; however, its applicability for the GDPR was confirmed in the *MICM* case by the CJEU. Mircom International Content Management & Consulting (M.I.C.M.) Limited v. Telenet BVBA, Case C-597/19, ¶ 106, [Ondernemingsrechtbank Antwerpen (Companies Court, Antwerp, Belgium)] June 17, 2021.

[287] Meta Platforms v. Bundeskartellamt, Case C-252/21, ¶ 119, Oberlandesgericht Düsseldorf [Higher Regional Court, Düsseldorf, Germany] July 4, 2023.

[288] *Id*. ¶ 120.

[289] *Id*. ¶ 130.

[290] *Id*. ¶ 126.

[291] *Id*. ¶ 112.

[292] Golden Data Law, *What is a "Supervisory Authority" (SA) under EU Data Protection Law?*, MEDIUM (Mar. 8, 2019), https://medium.com/golden-data/what-is-a-supervisory-authority-under-eu-data-protection-law-5ea69d5b0ea2 [https://perma.cc/W9HG-72ZP].

[293] GDPR, *supra* note 1, art. 9.

addresses.[294] Furthermore, in most Member States within the EU and other countries, there are Information Sharing and Analysis Centers ("ISACs") that facilitate the sharing of information relating to cybersecurity threats between public and private entities.[295] Would either of these actions contravene the GDPR? The Böck research team discusses this question from both the perspective of "public interest" and "commercial" research.[296] The former would relate to the ISACs, which operate on a non-profit basis and whose core function is the dissemination of threat knowledge. The latter would apply to private cybersecurity companies who conduct research for the development and advancement of their professional services and would likely be treated as an "ordinary" processing of data which has been discussed in detail already in this Paper. Private cybersecurity companies often release their research findings free of charge with the aim of public dissemination, and these releases, if they contain any personal data, may well fall under "public interest" research, although this has not been tested by the CJEU.

The Böck research team explains that, for public interest research, the appropriate lawful basis of processing would be either Article 6(1)(e) (public interest) or Article 6(1)(f) (legitimate interests).[297] In the *Endemol Shine* case, the CJEU confirmed that personal data can be shared publicly under Article 6(1)(e), so long as this is in the public's interest.[298] Legitimate interests have already been discussed in this Paper, and it is worth reiterating that the legitimate interests can be those of third parties.[299] The Böck research team also explains that Article 89 of the GDPR identifies scientific research as a "special regime" under the GDPR.[300] A researcher may not bypass the GDPR requirements but is granted a certain level of flexibility with regard to processing activities.[301] The authors also include guidelines for cybersecurity research; however, these relate only to botnet research activities where researchers may be granted access to a stream of personal data being generated

---

[294] ANDY GREENBERG, SANDWORM: A NEW ERA OF CYBERWAR AND THE HUNT FOR THE KREMLIN'S MOST DANGEROUS HACKERS, 19–20 (1st ed. 2019).

[295] *See, e.g.*, *Information Sharing and Analysis Centers (ISACs)*, ENISA, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing [https://perma.cc/9EVZ-EFBA] (last visited July 2, 2024).

[296] *See* Böck et al., *supra* note 43.

[297] *Id.*; Sarune Zybartaite, *Legitimate Interest Guide Under the GDPR*, GDPR REGISTER (Oct. 1, 2018), https://www.gdprregister.eu/gdpr/legitimate-interest-guide-under-the-gdpr/ [https://perma.cc/T4DD-DXEG].

[298] Endemol Shine Finland Oy, Case C-740/22, ¶ 49, Itä-Suomen hovioikeus [Court of Appeal, Eastern Finland, Finland] Mar. 7, 2024.

[299] *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC,* ARTICLE 29 DATA PROTECTION WORKING PARTY (Apr. 9, 2014), at 34, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf [https://perma.cc/T9ZH-PDLY] [hereinafter *Opinion on the Notion of Legitimate Interests*].

[300] Böck et al., *supra* note 43, § 4.2.

[301] *Id.*

by devices that are running malware.[302] It is unlikely this level of personal data would be shared by either ISACs or private cybersecurity companies disseminating threat research under the scenarios in question.

Finally, any controller or processor who relies on legitimate interests as their lawful basis for processing must demonstrate that the processing activity was both "necessary" (as per the second element of the *Rigas Satiksme* test), and "proportionate."[303] Proportionality is assessed *ex post*, and ACME Cyber Sentinel will need to demonstrate to the relevant supervisory agency that the specific processing activity was not excessive when weighed against the data subject's right to privacy. These requirements suggests that when ACME Cyber Sentinel relies on legitimate interests, it must demonstrate that no alternative means exist to achieve its legitimate interest without requiring the processing of the data subject's personal data—either at all, or to a lesser degree.

As part of this consideration, ACME Cyber Sentinel should consider if the particular and individual processing activity, when part of a series of processing activities relating to the data subject, may lead to inferences about the data subject that go beyond the objectives associated with the processing or lead to inferences deemed special categories of data.[304] If it believes this may be so, ACME Cyber Sentinel should reconsider the specific processing activity or use an alternative lawful basis for processing.

4. Can the personal data be transferred to ACME Cyber Sentinel?

In this alternative version of Scenario 2, where ACME Cyber Sentinel is outside the EU, ACME Cyber Sentinel is likely a controller. As was discussed in Scenario 1, if ACME Cyber Sentinel is a company headquartered in the United States, EU personal data is permitted to flow freely from the EU to the United States pursuant to the EU-U.S. Data Privacy Framework.[305] If ACME Cyber Sentinel is instead headquartered in a country without an adequacy decision,[306] it must use "supplementary measures" to provide a "contractual guarantee of an adequate level of protection against access by the public authorities of that third country to that data."[307] If ACME Cyber Sentinel fails

---

[302] *Id.* § 4.3.

[303] *Opinion on the Notion of Legitimate Interests*, *supra* note 299, at 34.

[304] *Id.* at 39.

[305] As was mentioned in Scenario 1, if a future challenge to this current United States adequacy decision was to invalidate the EU-U.S. Data Privacy Framework, then the United States would be viewed as a third country unless and until the United States could successfully negotiate another deal. *See* Chee, *supra* note 120.

[306] *See Adequacy Decisions*, *supra* note 107.

[307] Data Protection Comm'r v. Facebook Ireland & Schrems, Case C-311/18, ¶¶ 126, 133, 135, High Court, Ireland, July 16, 2020 (*Schrems II*); CHRISTAKIS, *supra* note 124.

to comply with these requirements, the controller may have to "suspend or end the transfer of personal data to the third country concerned."[308]

For transfers, it is important to recall one of the nuances related to pseudonymized data. In some circumstances, a data controller such as TechGuard can provide suitably pseudonymized data to ACME Cyber Sentinel for processing, assuming care has been taken to ensure that ACME Cyber Sentinel is unable to compel disclosure of the data subject. *Schrems I* and *Schrems II* raised concerns that governments in third countries could compel data from companies based outside the EU.[309] *Breyer* held that the mere existence of a single legal basis in which the third party can, even under remote circumstances, compel disclosure of the identity of the data subjects rebuts the presumption of anonymization.[310] The possibility of third country access to data may thus mean, depending on the facts, that this data could not be anonymous data under the transfer requirements.

In this Scenario, Business 1 (TechGuard) is headquartered in the EU. The specific country where Businesses 2 to 10 are headquartered could raise issues concerning the transfer of EU personal data for certain types of processing, particularly if any of these companies are headquartered in third countries. In Scenario 3, the Paper will revisit the potential issues raised by the headquarters of ACME Cyber Sentinel's clients.

Scenario 2 explores the legal risks of using EU data for the positive goal of identifying new cybersecurity threats, even if the amount of personal data being analyzed is quite limited. An important concern is that apparently de-identified data may be re-identified using information gathered from other sources. First, when a company, such as TechGuard, has had a breach (where the company is likely in need of cybersecurity services), it becomes more likely that ACME Cyber Sentinel will need to meet the standards for personal data processing due to the likelihood that outside information will transform non-personal data into personal data. A similar concern is that, as ACME Cyber Sentinel grows and has more clients, the chances increase that the non-personal data that the company gathers, such as security telemetry, is transformed into personal data because ACME Cyber Sentinel is more likely to re-identify data based on the greater number and types of data sources. Finally, when ACME Cyber Sentinel is non-EU-based, the company must ensure that it complies with additional requirements related to transfers of data but also may face a situation where it cannot treat pseudonymized data as anonymous data because of the practices of the government where ACME Cyber Sentinel is located.

---

[308] *Schrems II*, Case C-311/18 ¶ 135.

[309] *Id.*; Maximillian Schrems v. Data Protection Comm'r, Case C-362/14, High Court, Ireland, Oct. 6, 2015 (*Schrems I*).

[310] Patrick Breyer v. Bundesrepublik Deutschland, Case C-582/14, Bundesgerichtshof [BGH] [Federal Court of Justice] Oct. 19, 2016.

C. Analysis for Scenario 3

In Scenario 3, the AI cybersecurity tools for detection and prevention, vulnerability management, and identity management include the use of behavioral analytics. For example, behavioral analytics can help identify when an account is accessed from an unusual browser, device, or geographic location.[311] Also, behavioral analytics can be used to help confirm the identity of a customer or an employee, using techniques such as keystroke analysis.[312] As these examples suggest, AI cybersecurity tools utilizing behavioral analytics collect personal data and may collect sensitive personal data, like the typical locations of users (or of their devices) as well as patterns in keystrokes that can indicate certain medical conditions.[313] Scenario 3 focuses on the GDPR's regulation of the use of EU data, which is likely to be deemed personal data, to train, evaluate, and deploy models.[314] Scenario 4 discusses using trained AI cybersecurity tools to provide cybersecurity services to EU-based companies.

In Scenario 3, ACME Cyber Sentinel desires to use its gathered data to train, evaluate, and deploy new AI cybersecurity tools. In this scenario, the analysis of personal data and joint controllers follows that found in Scenario 2, so we dispense with the need to replicate that discussion.[315] As with the earlier scenarios, the legal requirements would be expected to become more complex if ACME Cyber Sentinel is non-EU-based, particularly if it is based in a country without an adequacy decision.

Utilizing the traditional interpretation of processing under the GDPR, the purpose for the processing in Scenario 3 would appear to be distinct from providing cybersecurity services to the ten clients, including TechGuard. The critical inquiry to consider under the GDPR is whether a lawful basis exists for processing this data. Under this traditional interpretation, the contract between ACME Cyber Sentinel and these clients may not provide the lawful basis for the purpose in this scenario, even though it did in Scenario 1 (training AI models may not be considered essential for the provision of the contract).

---

[311] Under the GDPR, geolocation data is generally considered personal data, but does not currently fall into a special category of data. *See* Zweifel-Keegan, *supra* note 53 ("The EU General Data Protection Regulation famously omits precise geolocation data from the list of special categories of personal data."); Sarfati, *supra* note 53.

[312] Yang et al., *supra* note 32; Canner, *supra* note 32; *see* Roy et. al., *supra* note 32.

[313] Wickramasinghe, *supra* note 34; *Behavioral Analytics*, *supra* note 34; *What is AI-Powered Behavioral Analysis In Cybersecurity*, *supra* note 34.

[314] *See* Clark et al., *supra* note 162.

[315] *See Guidelines on the Concepts of Controller and Processor*, *supra* note 57; *see also* Helena Engfeldt & Jonathan Tam, *Can Processors Use Data to Train AI, Improve Products While Remaining a Processor?*, IAPP (July 3, 2024), https://iapp.org/news/a/can-processors-use-data-to-train-ai-improve-products-while-remaining-a-processor-?mkt_tok=MTM4LUVaTS0wNDIAAAGUGLo2t8I3bXz8T9CCCNycw1Y-Zt4X7nBQ_GovtrODOhUyIP0Rk_mfHmi491czIKfj-60EdAcyLgzCGmVnKOpqxewZUyAl4ApGKGJlUb6V5rbI [https://perma.cc/B66X-G4TG].

Under such reasoning, as with Scenario 2, another lawful basis would need to be identified, which could lead to the need for this EU data to be anonymized, or perhaps pseudonymized (as discussed in the legal analysis of Scenario 2), to be used in this manner.[316] It is worth pointing out that anonymized data may have limited use for the purpose in this scenario, such as in particular AI cybersecurity tools that utilize behavioral analytics.

Importantly, it is unclear how this traditional approach to processing will be adopted in the EU for AI tools—as the CJEU has yet to rule on topics related to AI and data protection.[317] Recent commentary from several DPAs suggests that the GDPR's application to use AI tools will likely be tailored to the unique circumstances of this evolving technology.[318] For example, the Hamburg DPA suggests that the use of an AI model would itself not fall within the scope of the GDPR, meaning that merely using such a model would not be considered processing of personal data.[319] The Hamburg DPA even points out that "[p]otentially unlawful processing of personal data during the training of a model does not affect the legality of using said model."[320]

For Scenario 3, ACME Cyber Sentinel trains, evaluates, and deploys AI cybersecurity tools. The pertinent question is, therefore, whether and how the GDPR applies to the development of an AI tool. As one early case, which may or may not be followed in other cases on this rapidly-developing topic, the Hamburg DPA found that training a large language model ("LLM")[321] using personal data would fall within the scope of the GDPR and any data protection violations during the training of an LLM would be "attributable . . . exclusively to model's developer."[322] The Hamburg DPA also noted that, when an entity deploys and fine-tunes the LLM, that entity must comply with the GDPR and must have a legal basis for any personal data used in the fine-tuning.[323] If this view of the Hamburg DPA is followed generally, it would

---

[316] *See generally* Bock, et al., *supra* note 43.

[317] *See* HAMBURG COMM'R DATA PROT. & FREEDOM OF INFO., DISCUSSION PAPER: LARGE LANGUAGE MODELS AND PERSONAL DATA 4–6 (2024), https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Discussion_Paper_Hamburg_DPA_KI_Models.pdf [https://perma.cc/SU4J-B4G8].

[318] *See id.*; *Subcontractors: The Reuse of Data Entrusted by a Data Controller*, *supra* note 255; *see also* DATATILSYNET, USE OF ARTIFICIAL INTELLIGENCE IN THE PUBLIC SECTOR (2023) (translated from Danish), https://www.datatilsynet.dk/Media/638321084132236143/Offentlige%20myn-digheders%20brug%20af%20kunstig%20intelligens%20-%20Inden%20I%20g%C3%A5r%20i%20gang.pdf [https://perma.cc/RYZ4-V76Y].

[319] HAMBURG COMM'R DATA PROT. & FREEDOM OF INFO., *supra* note 317; *see* DATATILSYNET, *supra* note 318, at 7.

[320] HAMBURG COMM'R DATA PROT. & FREEDOM OF INFO., *supra* note 317, at 8.

[321] The Hamburg DPA distinguishes between an AI system and one of its component parts, an LLM. *Id.* at 2. The Hamburg DPA notes that it does not fully "evaluate the processing activities in the entire AI system." *Id.*

[322] *Id.* at 8.

[323] *Id.* at 8–9.

appear that ACME Cyber Sentinel would be responsible for complying with the GDPR in training the AI cybersecurity tools as well as when fine-tuning these tools.

This subpart now turns to the potential issues raised by the headquarters of ACME Cyber Sentinel's clients. While Business 1 (TechGuard) is EU-based, it is insightful to imagine Businesses 2 to 10 as headquartered in one or more non-EU third countries. ACME Cyber Sentinel gathers personal data from Businesses 1 to 10, including EU personal data from TechGuard, to train and evaluate new AI cybersecurity tools, where ACME Cyber Sentinel then deploys these updated tools to all ten businesses.[324]

Again, applying a traditional interpretation to processing under the GDPR, the activity of deploying the updated AI cybersecurity tools, that are trained on EU personal data, to Businesses 2 to 10 could potentially be deemed a transfer of this personal data to one or more third countries. Under this interpretation, these transfers could be particularly problematic if a DPA imposed the "zero-risk" approach examined by European scholar Christakis.[325]

To date, however, the CJEU has not ruled that AI models store personal data—one of the critical steps in a determination that deploying an updated tool constitutes a transfer of EU personal data. The Hamburg DPA states that an LLM "does not store personal data."[326] The Hamburg DPA's conclusion would seem to suggest that the use of EU personal data to train the AI model in Scenario 3 might not lead to a situation where ACME Cyber Sentinel's use of the updated AI cybersecurity tools would constitute a transfer of the EU personal data to Businesses 2 to 10. Notably, the use of personal data for the purpose described in this subpart is an area where the legal requirements are still developing in the EU, and around the world.

D. Analysis for Scenario 4

In Scenario 4, the facts of Scenario 1 where ACME Cyber Sentinel provided cybersecurity services to TechGuard apply. In the earlier scenario, ACME Cyber Sentinel was likely acting as a processor. Scenarios 2 and 3 explored how ACME Cyber Sentinel probably acts as a controller for the limited amount of data it collects related to potential cyber threats as well as for the AI cybersecurity tools that it trains, evaluates, and deploys concerning

---

[324] To the extent that the countries where Businesses 2 to 10 are headquartered have data protection and/or AI regulations that impact this assessment, these requirements are beyond the scope of this Paper.

[325] This approach is detailed in Scenario 1. CHRISTAKIS, *supra* note 124.; *see Techniques, Tactics, and Procedures*, *supra* note 5, at 11.

[326] HAMBURG COMM'R DATA PROT. & FREEDOM OF INFO., *supra* note 317, at 5. The Hamburg DPA stated, "Although it has been observed that fine-tuned LLMs are occasionally made to reproduce training data through privacy attacks, it is doubtful whether this type of extraction validates the legal conclusion that personal data is stored in the LLM." *Id.*

newly identified threats. Scenario 4 re-examines the original set of circumstances when ACME Cyber Sentinel provided cybersecurity services to TechGuard, focusing on the fact that ACME Cyber Sentinel now utilizes AI cybersecurity tools to provide these services.

As in Scenario 1, ACME Cyber Sentinel collects personal data or sensitive personal data, such as current locations of users, or of their devices, or the keystrokes of customers or employees when these AI cybersecurity tools are used to provide its cybersecurity services.

With regard to the use of AI with EU individuals and their data, questions arise regarding whether the decisions at issue (those being undertaken by the AI systems) are permitted and whether they are regulated. Concerning the GDPR, individuals have a right against automated decision-making. As discussed above, however, this right likely does not apply to the type of decisions currently made by AI cybersecurity tools. Under the EU AI Act, an AI system is deemed to be high risk if the decisions made by the system relate to "health, safety, or fundamental rights," such as in "medical devices, vehicles, emotion recognition systems, and law enforcement."[327] Again, AI cybersecurity tools generally do not appear to make these types of decisions.

When looking at the responsibilities of ACME Cyber Sentinel and TechGuard in this scenario, it is important to examine the different components of the AI cybersecurity tools—the inputs, the outputs, and the models themselves.[328] Although the Hamburg DPA indicates that the use of an AI model probably does not fall within the scope of the GDPR (because it would not be seen to store personal information from a legal perspective),[329] the Hamburg DPA explains that "when an AI system processes personal data, particularly in its output or database queries, the controller must fulfill data subject rights."[330] Thus, the controller in this scenario will likely need to address data subject rights related to inputs and outputs. Whether this controller would be TechGuard, ACME Cyber Sentinel, or both will depend on the relationship between the two (as explained in detail in the earlier scenarios of this Paper). As with Scenarios 1, 2, and 3, the legal requirements become more complex if ACME Cyber Sentinel is non-EU-based, particularly if it is based in a country without an adequacy decision.

The future use of behavioral analytics in AI cybersecurity tools for detection and prevention, vulnerability management, and identity management could present issues under the GDPR and the EU AI Act. Technologies developed to verify identity could include the use of heartbeat data, which could reveal certain medical conditions and be viewed as "biometric data [being used] for the purpose of uniquely identifying a natural

---

[327] EU AI Act, *supra* note 2, art. 86.

[328] HAMBURG COMM'R DATA PROT. & FREEDOM OF INFO., *supra* note 317, at 2.

[329] *See id.*; *see* DATATILSYNET, *supra* note 318, at 7

[330] HAMBURG COMM'R DATA PROT. & FREEDOM OF INFO., *supra* note 317, at 9.

person,"[331] or the use of eye movement, which could be related to biometric data under the GDPR's special categories of personal data.[332] Unlike keystroke analysis, heartbeat data is generally medical in nature and most likely falls under a special category of personal data in the GDPR. For eye movement (and to a lesser extent, heartbeat data), the EU AI Act's unacceptable risk AI systems include "emotion recognition systems" at work or in school that identify or infer "emotions or intentions" of individuals based on biometric data.[333] An AI cybersecurity tool using eye movements to verify an employee's identity could potentially fall into this prohibited category. The same tool used to verify a customer's identity has the potential to fall into the heavily regulated high-risk AI category under the EU AI Act.

The actual use of ACME Cyber Sentinel's AI cybersecurity tools may be lawful under the analysis of Scenario 1. Certain tools, particularly those that use biometrics or other behavioral analytics, could be more problematic to deploy in the EU. As with Scenario 3, the legal requirements regarding the training and use of AI systems in the EU and worldwide are developing. ACME Cyber Sentinel would likely benefit from voluntarily adhering to industry codes of conduct, as discussed in the EU AI Act.

V. CONCLUSION

Cybersecurity is both a worthwhile goal for society and a requirement for data protection under the GDPR.[334] While privacy and cybersecurity often complement each other, there are instances when they can be at odds, particularly when data protection limitations on processing personal data can

---

[331] GDPR, *supra* note 1, arts. 9(1), 4(14); BIOMETRICS INST., *Types of Biometrics: Heartbeat – Key Considerations*, https://www.biometricsinstitute.org/types-of-biometrics-heartbeat-key-considerations/#:~:text=Heartbeat%20biometric%20identification%20is%20considered,the%20most%20widely%20used%20currently [https://perma.cc/L6UM-UD4U] (last visited July 3, 2024); *How Heartbeat Biometrics Could Be the Next Big Thing?*, ARATEK (Feb. 24, 2023), https://www.aratek.co/news/how-heartbeat-biometrics-could-be-the-next-big-thing#:~:text=Five%20characteristics%20are%20considered%20%E2%80%94%20dynamics,96.6%20per%20cent%20in%20experiments [https://perma.cc/FWS6-54VE]; *Method and Device for Biometric Verification and Identification,* NASA, https://technology.nasa.gov/patent/TOP2-202 [https://perma.cc/J8WZ-8DGM] (last visited July 2, 2024).

[332] GDPR, *supra* note 1, arts. 9(1), 4(14); Christina Nunez, *How Eye Movement Could Unlock New Levels of Computer Security,* COLBYNEWS (Nov. 23, 2021), https://news.colby.edu/story/can-eye-movement-unlock-new-levels-of-security/ [https://perma.cc/W6LH-84Y7]; *see* Chiara Gald et al., *Eye Movement Analysis for Human Authentication: A Critical Survey*, 84 PATTERN RECOGNITION LETTERS 272 (2016); Jacob Leon Kröger et al., *What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking,* 576 PRIVACY & IDENTITY 226 (2020).

[333] EU AI Act, *supra* note 2, art. 3(39).

[334] GDPR, *supra* note 1, art. 5(1)(f).

reduce the effectiveness of cybersecurity protections for personal data.[335] This Paper analyzed four important scenarios where cybersecurity services were provided, both with and without AI, to highlight current doctrine and possible issues under EU law. The Paper also assumed that ACME Cyber Sentinel complies with other requirements of EU law, such as being transparent with clients and individuals about their data practices, using the minimum necessary personal data, and avoiding marketing based on profiles of individuals.

The processing of personal data is generally not the main focus for companies providing cybersecurity services. These companies, like ACME Cyber Sentinel, do not primarily engage in the typical processor behavior of "processing personal data on the controller's behalf."[336] When it comes to whether a company like ACME Cyber Sentinel is functioning as a processor or a controller, the EDPB points out, from a practical perspective, "where the provided service is not specifically targeted at processing personal data . . . , the service provider may be in a position to independently determine the purposes and means of that processing which is required in order to provide the service."[337] In other words, this type of processing can appear to be the work of a controller. The analysis, however, does not end with this initial evaluation. The EDPB goes on to explain that "a service provider may be acting as a processor even if the processing of personal data is not the main or primary object of the service," so long as the client of the service determines the purposes and means of the processing.[338] For companies like ACME Cyber Sentinel, the nature of their services likely means that the full assessment of whether they act as a processor or a controller relies on complex analysis. These companies reduce compliance risk when they carefully document their client relationships in written agreements and work diligently to ensure that both parties follow the parameters set forth in these written agreements.

There are two additional takeaways from the Paper's analysis—one focusing on providing cybersecurity services to EU-based businesses and the other raising concerns for maintaining state-of-the-art cybersecurity services and tools, regardless of geography. First, cybersecurity companies, whether based inside or outside the EU, can provide many cybersecurity services to EU-based businesses, including services using AI cybersecurity tools. For non-EU cybersecurity companies, additional protections must be implemented to address the legal concerns around "transfers" of personal data.

---

[335] For discussion of the possibility of privacy and cybersecurity being at odds, see *Organizational Effects*, *supra* note 5.

[336] *Guidelines on the Concepts of Controller and Processor*, *supra* note 57, ¶ 76.

[337] *Id.* ¶ 82.

[338] *Id.* ¶ 83. In a third example, an IT consultant is hired to fix a bug in software. According to the example, "The IT-consultant is not hired to process personal data, and Company ABC determines that any access to personal data will be purely incidental and therefore very limited in practice." *Id.* Under this set of facts, the IT consultant is deemed to be neither a processor nor a controller. *Id.*

These additional protections may require supplementary measures and may be difficult to meet for cybersecurity companies processing the data in third countries that lack an adequacy decision. Second, the legal protections in place for personal data in the EU may make it difficult to utilize this data for some positive cybersecurity outcomes for the public, such as to identify new cybersecurity threats or to train the algorithms used in machine learning, AI and other cybersecurity tools. In essence, EU-based businesses can enter into contracts with cybersecurity companies to protect EU data with state-of-the-art cybersecurity services and tools, but it becomes more difficult to locate a lawful basis for using EU data to identify new cybersecurity threats or to train new machine learning, AI and other cybersecurity tools. In game theory, this is known as the "free rider problem"—a term that describes a situation where people benefit from the information provided by others while not sharing their own information.[339]

More attention may be needed to receive authoritative guidance on when and whether identifying new threats or training algorithms are considered necessary for performance of the contract for cybersecurity services. Although privacy-enhancing technologies ("PETs")—such as federated ML, differential privacy, or homomorphic encryption—may permit limited use of EU personal data for cybersecurity purposes (other than providing cybersecurity services) to provide at least a partial resolution to the free rider problem,[340] there are limits to the uses of PETs to solve the legal issues where cybersecurity can come into conflict with data protection. In identifying new cybersecurity threats or to training new machine learning, AI and other cybersecurity tools, there likely are instances where defenders need access to the original personal data to accomplish the goals of cybersecurity. To conclude, it is clear that further clarification from EU decision-makers would help define whether and how access to personal data will be lawful for cybersecurity purposes.

---

[339] Juan Trocoso-Pastoriza, et al., *Orchestrating Collaborative Cybersecurity: A Secure Framework for Distributed Privacy-Preserving Threat Intelligence*, ARXIV (Sept. 6, 2022), https://arxiv.org/abs/2209.02676 [https://perma.cc/3D6S-J9BF]; Alain Mermound, et al., *To Share or Not to Share: A Behavioral Perspective on Human Participation in Security Information Sharing*, 5 J. CYBERSECURITY 1 (2019).

[340] Trocoso-Pastoriza, *supra* note 339.