BREACHING THE UNKNOWN: FIVE LESSONS FROM GDPR ARTICLE 32 FINES

GABY VELKES*

I. INTRODUCTION

Regulation (EU) 2016/679 of the European Parliament and the Counsel, the new General Data Protection Regulation (GDPR), went into effect on May 25, 2018, replacing the previous E.U. 1995 data protection directive.[1] The new GDPR represents a large departure from the previous directive, aimed at affording additional online data protections yet creating a vast space of regulatory uncertainty about what it means for businesses to be complaint with the GDPR.[2] One major area of uncertainty is how regulators will enforce the GDPR through Article 32. Article 32 addresses the security of processing personal data and requires:

> [T]aking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk . . . .[3]

Article 32 violations of the GDPR have been responsible for a significant portion of penalties that E.U. authorities have imposed under the GDPR.[4] Article 32 also includes a nonexhaustive list of technology-neutral measures aimed at reasonable data security, such as "pseudonymisation and encryption of personal data," but does not prescribe specific requirements or examples of what constitutes sufficient GDPR-compliant data processing.[5] Although an external data breach may

---

* This online annotation was written in the course of the author's tenure as a Staff Editor on the *N.Y.U. Journal of International Law & Politics*.

[1] Matt Burgess, *What Is GDPR? The Summary Guide to GDPR Compliance in the UK,* WIRED (Jan. 21, 2019), https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.

[2] *See* Jonathan Greig, *Companies Still Unprepared for GDPR Rule Changes and Potential EU Data Breaches*, TECHREPUBLIC (Sept. 16, 2019), https://www.techrepublic.com/article/companies-still-unprepared-for-gdpr-rule-changes-and-potential-eu-data-breaches ("A new survey finds many companies are still in the dark about GDPR compliance.").

[3] Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 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 Act), art. 32(1), 2016 O.J. (L 119/1) [hereinafter GDPR].

[4] GDPR ENFORCEMENT TRACKER, http://www.enforcementtracker.com (last visited Nov. 15, 2019) (indicating that of the 109 reported fines and penalties under the GDPR, thirty involved Article 32).

[5] GDPR, *supra* note 3, art. 32(1).

be indicative of a failure of the duty to securely process data, many of the Article 32 enforcement decisions from the first year and a half of the GDPR regime appear to be aimed at *preemptively* preventing the occurrence of such breaches, rather than functioning as a reactive measure.[6]

These early Article 32 fines provide a useful lens into what, in practice, constitutes insufficient data processing, and thus begin to illuminate what qualifies as appropriate data security under the GDPR.[7] Analysis of these matters reveals five important lessons for organizations trying to comply with GDPR Article 32 regulations: (1) the importance of password security, (2) the necessity of proper documentation of security protocols, (3) the emphasis on tracking user access as well as (4) preventing unauthorized access in the first instance, and (5) the emerging doctrine surrounding the legal duty to safeguard personal data. It can be predicted that these five areas may prove to represent the bulk of future Article 32 enforcement efforts, and organizations should respond accordingly.

II. PASSWORD SECURITY

Several of the early GDPR Article 32 fines emphasize the importance of password security and suggest several protective measures that may be necessary for GDPR compliance. The first GDPR fine that Germany issued addressed violations of Article 32 by the chat app Knuddels.[8] This case highlights the unequivocal stance of Germany's Baden-Wuerttemberg Data Protection Authority: "By storing passwords in clear text, [Knuddels] knowingly violated its duty to ensure data security in the processing of personal data . . . ."[9] It is thus clear that storing passwords in

---

[6] Vera Cherepanova, *GDPR Enforcement Report (May 2019)*, FCPA BLOG (May 14, 2019), https://www.fcpablog.com/blog/2019/5/14/gdpr-enforcement-report-may-2019.html.

[7] Although not all Article 32 actions thus far have addressed online activity, the majority appear to be focused on online data, and so this annotation will focus primarily on those actions. *See, e.g.*, *A New Fine for the Application of GDPR*, NAT'L SUPERVISORY AUTHORITY FOR PERS. DATA PROCESSING, https://www.dataprotection.ro/index.jsp?page=O_noua_amenda_GDPR&lang=en (last visited Nov. 15, 2019) (describing a fine imposed on World Trade Center Bucharest S.A. due to a "breach of personal data security [that] consisted in the fact that [sic] a printed paper list used to check the customers attending breakfast and which contained personal data of 46 clients accommodated at the hotel").

[8] Ionut Ilascu, *First GDPR Sanction in Germany Fines Flirty Chat Platform EUR 20,000*, BLEEPING COMPUTER (Nov. 23, 2018), https://www.bleepingcomputer.com/news/security/first-gdpr-sanction-in-germany-fines-flirty-chat-platform-eur-20-000/.

[9] Richard Chirgwin, *'Cuddly' German Chat App Slacking on Hashing Given a Good Whacking Under GDPR: €20k Fine*, REG. (Nov. 23, 2018), https://www.theregister.co.uk/2018/11/23/knuddels_fined_for_plain_text_passwords.

clear text will *not* be considered an appropriate data standard, despite the absence of an explicit requirement stating otherwise in Article 32.[10]

The Commission Nationale de l'Informatique et des Libertés (CNIL), the French authority charged with GDPR enforcement, gave specific directives regarding password protection enhancements in its sanction deliberation against Uniontrad.[11] In its sanction, the CNIL mandated the implementation of a new password policy; however, rather than specify a password protocol, the decision included several options for Uniontrad to pursue.[12] Although it committed several other GDPR violations, Uniontrad's failure to implement the CNIL-suggested password security measures was cited as one of the primary reasons for the action under Article 32, emphasizing the importance of basic password security under the GDPR.[13] The same password requirements are reiterated in a later decision against Active Insurances.[14] In that decision, the CNIL noted that "insufficient robustness of the passwords does not make it possible to ensure the security of the data processed by the company and to prevent brute force attacks which . . . lead, thus, to a compromise of the associated accounts and the personal data they contain."[15]

The CNIL password suggestions in both the Uniontrad and Active Assurances deliberations narrow what appropriate password security may be necessary for GDPR compliance. Although these protocols may not definitively serve as a defense, they are indicative of the level of technical

---

[10] GDPR, *supra* note 3, art. 32. Suggested actions include, when appropriate: "(a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing." GDPR, *supra* note 3, art. 32(1).

[11] Commission Nationale de l'Informatique et des Libertés, June 13, 2019, *Délibération no. SAN-2019-006 du 13 juin 2019 [Deliberation SAN-2019-006 of June 13, 2019]*, LEGIFRANCE (June 18, 2019) [hereinafter CNIL SAN-2019-006], https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000038629823 (Fr.).

[12] *Id.* These options included that: "[P]asswords consist of at least 12 characters, containing at least one uppercase letter, one lowercase letter, one number, and one special character; passwords are composed of at least eight character, containing three of the four categories of characters (capital letters, lowercase letters, numbers and special characters) and are accompanied by a complementary measure such as the account access delay after several failures, (temporary suspension of access, the duration of which increases as attempts are made), the setting up of a mechanism to guard against automated and intensive attempts (eg [sic] captcha) and / or blocking the account after several unsuccessful authentication attempts (up to ten); storing passwords in a hashed form (for example, using the SHA256 algorithm with the use of a salt); [and] in any case, the passwords must be regularly renewed . . . ." *Id.* (translation provided by author).

[13] *Id.*

[14] Commission Nationale de l'Informatique et des Libertés, ¶ 53, July 18, 2019, *Délibération No. SAN-2019-007 du 18 juillet 2019 [Deliberation No. SAN-2019-006 of July 18, 2019]*, LEGIFRANCE (July 25, 2019), https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000038810992 (Fr.).

[15] *Id.* ¶ 50 (translation provided by author).

safeguards expected under the new regulation. These decisions strongly imply that under Article 32, passwords should be regularly renewed and sufficiently complex or guarded by appropriate technical safeguards.

Overall, these cases demonstrate that basic password security measures are a cornerstone of appropriate data security. Passwords should never be stored in clear text, and should ideally incorporate the technical safeguards that the CNIL emphasized in the French fine deliberations as a precaution, or companies may otherwise face disciplinary action.

III. DOCUMENTATION OF DATA SECURITY PROCEDURES

Portugal's first GDPR fine appears to be in response not to a breach of data, but rather was a proactive enforcement against subpar data security practices. [16] The Comissão Nacional de Protecção de Dados, the Portuguese agency charged with enforcing certain GDPR provisions, focused on the offending hospital's lack of documentation for standardized data access procedures, especially because of the highly sensitive nature of the data in question.[17] This action reveals the importance of the presence of documented data security procedures, especially when the data being processed is highly sensitive.

IV. TRACKING USERS TO DISCOURAGE UNNECESSARY ACCESS

The need for user access tracking is consistently cited as a means to identify illegal access while user authentication, discussed below, is seen as a preventive measure to protect against such access. While preventing unauthorized access in the first instance is ideal, tracking user access is also necessary to ensure that even authorized users do not access unauthorized data. For example, just because an employee might have access to the employer's network, it doesn't mean the employee has access to coworkers' files.

In the aforementioned action against Uniontrad, the CNIL noted that the company had "not put in place measures to ensure the traceability of individual accesses to the shared professional mailbox," and that "it is important to ensure that users are authenticated through individual accounts before accessing the data."[18] This emphasizes the CNIL's belief in the necessity of appropriate user access tracking.

Furthermore, the Dutch Data Protection Authority (AP) decision against Haga Hospital was not in response to a large-scale breach, but rather was the result of staff's unnecessary access to a well-known Dutch person's medical records.[19] The AP noted that the hospital had insufficient

---

[16] Ana Menezes Monteiro, *First GDPR Fine in Portugal Issued Against Hospital for Three Violations,* INT'L ASS'N PRIVACY PROFS. (Jan. 3, 2019), https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations.

[17] *Id.*

[18] CNIL SAN-2019-006, *supra* note 11 (translation provided by author).

[19] *Haga Beboet Voor Onvoldoende Interne Beveiliging Patiëntendossiers [Haga Fined for Insufficient Internal Security of Patient Records]*, AUTORITEIT

security measures for tracking access to medical files, which would have ensured that any unauthorized action could be identified and punished.[20]

In the decision against the political party Associazione Movimento 5 Stelle in Italy, the sharing of user credentials and failure to limit data access for certain users was cited as clearly falling below the minimum security measures required by law.[21] The failure to track user access was the main rationale for the decision to impose fines against Associazione Movimento 5 Stelle.[22]

These cases clearly highlight the emphasis European regulators place on the importance of tracking user access. Wholesale abrogation of this duty, as shown, can clearly lead to violations under Article 32.

V. USER AUTHENTICATION

User authentication also represents an important preventive measure to ensure that unauthorized users are unable to gain access to protected data in the first place. In its decision against Haga Hospital, the AP noted that "[g]ood security requires authentication that involves at least two factors."[23] Although this is in the context of highly sensitive medical data, it is significant that the AP notes that the lack of two-factor authentication procedures is indicative of "insufficient security measures."[24]

Norway's first GDPR fine also involved a violation of Article 32 for "insufficient security measures" for protecting personal data, this time the data of students and employees in the Bergen municipal school district.[25] In its final decision, the Norwegian Data Protection Authority noted that the proposed introduction of a two-factor authentication system would raise data security to the appropriate standards for user authentication.[26]

PERSOONSGEGEVENS [DUTCH DATA PROTECTION AUTHORITY], (July 16, 2019), https://autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-pati%C3%ABntendossiers [hereinafter *Haga Fined for Insufficient Security*] (Neth.); Janene Pieters, *Hague Hospital Fined €460,000 for Not Protecting Patient's Privacy*, NL TIMES (July 16, 2019), https://nltimes.nl/2019/07/16/hague-hospital-fined-eu460000-protecting-patients-privacy.

[20] Pieters, *supra* note 19.

[21] *Provvedimento Su Data Breach: Il Garante Per La Protezione Dei Dati Personali [Ruling on Data Breach: The Guarantee for the Protection of Personal Data]*, GARANTE PER LA PROTEZIONE DEI DATI PERSONALI [ITALIAN DATA PROTECTION AUTHORITY] (Apr. 4, 2019), https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9101974 (It.).

[22] *Id.*

[23] *Haga Fined for Insufficient Security*, *supra* note 19 (translation provided by author).

[24] *Id.* (translation provided by author).

[25] *Administrative Fine of €170,000 Imposed on Bergen Municipality*, EUR. DATA PROTECTION BOARD (March 19, 2019), https://edpb.europa.eu/news/national-news/2019/administrative-fine-eu170000-imposed-bergen-municipality_en.

[26] Stine Dahl, *Endelig Vedtak om Gebyr til Bergen Kommune [Final Decision on Fee to Bergen Municipality]*, DATATILSYNET (Mar. 19, 2019), https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-20192/endelig-vedtak-om-gebyr-til-bergen-kommune (Nor.).

In another instance, a CNIL investigation revealed the existence of a security defect on the real estate company Sergic's website that allowed documents (including rental applications) to be freely accessible through a simple manipulation of the company's URL.[27] The CNIL stated that "exposure of personal data without prior access control is identified as one of the most widespread vulnerabilities."[28] The CNIL also noted that a user authentication procedure, which the website lacked, was an "essential precautionary measure" that would have greatly reduced the possibility of a data breach.[29]

These cases reveal that lack of user authentication is often cited as grounds for a decision that an organization failed to meet appropriate data security standards. Similar to user access tracking, user authentication is seen as a necessary precaution against unauthorized user access, and lack of two-factor authentication, or some other equally robust security mechanism, may leave a company vulnerable to GDPR action.

VI. MOVING FORWARD: THE LEGAL DUTY TO SAFEGUARD PERSONAL DATA

Although the discussed cases primarily concerned failures to implement *preventative* security measures, GDPR regulators are no less disincentivized to fine organizations whose poor data processing have led to major breaches. Recently, the Information Commissioner's Office (ICO), the UK agency charged with enforcing GDPR regulations, has announced an intention to fine both British Airways and Marriott International in response to large personal data breaches.[30] These proposed fines would represent the largest fines in the GDPR's history, and may indicate an increasing willingness of regulators to impose significant fines on major data breach offenders.[31] While the Marriott fine is in response to the exposure of approximately 339 million guest records, the ICO framed

---

[27] Commission Nationale de l'Informatique et des Libertés, May 28, 2019, *Délibération No. SAN-2019-005 du 28 mai 2019 [Deliberation No. SAN-2019-005 of May 28, 2019]*, LEGIFRANCE (June 6, 2019), https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000038552658 (Fr.).

[28] *Id.* ¶ 34 (translation provided by author).

[29] *Id.* ¶ 33 (translation provided by author).

[30] *Intention to Fine British Airways £183.39m Under GDPR for Data Breach*, INFO. COMMISSIONER'S OFF. (July 8, 2019), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways [hereinafter *Intention to Fine British Airways*]; *Statement: Intention to Fine Marriott International, Inc More Than £99 Million Under GDPR for Data Breach*, INFO. COMMISSIONER'S OFF. (July 9, 2019), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach [hereinafter *Intention to Fine Marriott International*].

[31] Mark Rogan, *GDPR's Big Moment Has Just Arrived—With a $228 Million Data Breach Fine,* CPO MAG. (Sept. 12, 2019), https://www.cpomagazine.com/data-protection/gdprs-big-moment-has-just-arrived-with-a-228-million-data-breach-fine.

the incident as a failure of the legal duty to ensure data security.[32] The ICO invoked similar language regarding the duty to safeguard personal data with respect to the British Airways exposure of approximately 500 thousand customers.[33] So, while some seek reactive action against data breaches, it is still framed as a failure of the duty established by Article 32 to implement appropriate data security safeguards, and not simply as a punitive response to the breach.

As the doctrine surrounding the duty to safeguard personal data emerges, it is clear that it includes strong basic safety measures, specifically password security, documentation of protocols, and user authentication and tracking. In the recent decision of Poland's Office for Personal Data Protection to fine Morele.net, these principles are brought to life. The President of the Office for Personal Data Protection noted that "access control and authentication are the basic security measures to protect against unauthorized access to the IT system used to process personal data."[34] Although this action was in response to a data breach, the President was careful to note that the breach of confidentiality "should be considered from the perspective of two events: obtaining unauthorized access to . . . and obtaining the data of all customers from the Company's database system."[35] Just because a company has not been the target of a large breach, does not guarantee immunity from GDPR action. Most importantly, this case and others demonstrate that the duty to safeguard personal data may be violated whenever data practices fail to meet these basic security measures. Overall, although the GDPR is still in its infancy, and GDPR-related regulatory action still developing, the decisions available provide insight into the future of regulatory action under the GDPR. Regulators will likely continue to place a premium on enforcing preventative measures, effectively inducing the implementation of strong monitoring systems, rather than primarily focusing ex post on entities that have suffered breaches.

---

[32] *See Statement: Intention to Fine Marriott International, Inc More Than £99 Million under GDPR for Data Breach*, *supra* note 30 ("Personal data has a real value so organisations have a legal duty to ensure its security, just like they would do with any other asset. If that doesn't happen, we will not hesitate to take strong action when necessary to protect the rights of the public.").

[33] *See Intention to Fine British Airways*, *supra* note 30 ("People's personal data is just that—personal. When an organisation fails to protect it from loss, damage or theft it is more than an inconvenience. That's why the law is clear—when you are entrusted with personal data you must look after it. Those that don't will face scrutiny from my office to check they have taken appropriate steps to protect fundamental privacy rights.").

[34] Decision ZSPR 421.2.2019 of September 10, 2019, of the President of the Personal Data Protection Office, https://uodo.gov.pl/decyzje/ZSPR.421.2.2019 (translation provided by author) (Pol.).

[35] *Id.* (translation provided by author).