pillsbury

DATA PRIVACY AND COMPLIANCE IN THE AGE OF FULLY HOMOMORPHIC ENCRYPTION (FHE)

GDPR, CCPA AND BIPA

By Cassie Lentchner and Steven Farmer

Privileged and Confidential

CONTENTS

DATE
AUGUST 1, 2020

1. EXECUTIVE SUMMARY

Private Identity LLC asked us to consider whether the company's Cloud Biometric MFA fully homomorphic encryption ("FHE") cryptography system (the "Cloud Biometric MFA system") is subject to EU and US privacy laws and obligations and to what extent the Cloud Biometric MFA system helps further the data protection principles that form the basis for processing personal data (including biometric data) with respect to the General Data Protection Regulation ("GDPR"), the California Consumer Privacy Act ("CCPA") and the Illinois Biometric Information Privacy Act ("BIPA").

FHE enables encrypted match and search operations on encrypted data without allowing any third party to observe the actual data. The Cloud Biometric MFA system enables the individual end user to generate an FHE payload using his/her own biometrics. This FHE payload is then transmitted to Private Identity to support encrypted enrollment, match and search operations.

On the basis of the information provided to us and reviewed, we have concluded that the FHE payload is anonymized data. The FHE payload is a globally unique positional array that does not contain biological or behavioral characteristics, imagery or a template of any physiological, biological or behavioral trait.

Additionally, instead of using personal data, the Cloud Biometric MFA system generates a universally unique identifier ("UUID") to label each end user. This UUID cannot be tied back to an individual/end user by Private Identity. Therefore, we conclude that the UUID is also anonymized data.

Accordingly, we find that the FHE payloads and UUIDs are not "personal data" or "biometric data" under the GDPR, "personal information" or "biometric information" under the CCPA, and not "biometric identifiers" or "biometric information" under the BIPA. As such, these laws do not apply to the Cloud Biometric MFA system.

We have also concluded that the Cloud Biometric MFA system seeks to advance data protection principles underlying the data protection laws. For example, the Cloud Biometric MFA system fulfills the GDPR, CCPA and BIPA's regulatory and policy goals by minimizing the need to process unnecessary categories of personal data.

Moreover, because he Cloud Biometric MFA system processes only anonymized data, as described above, this eliminates the data subject's rights that would otherwise arise when personal data is being processed.

Finally, we find the loss of any FHE payloads and UUIDs would not constitute a breach of biometric data or personal data because they do not constitute personal data.

2. BACKGROUND

Private Identity LLC asked us to consider whether the company's Cloud Biometric MFA fully homomorphic encryption (FHE) cryptography system (the "Cloud Biometric MFA system") is subject to EU and US privacy laws and obligations and to what extent the Cloud Biometric MFA system helps further the data protection principles that form the basis for processing personal data (including biometric data) with respect to the General Data Protection Regulation (EU) 2016/679 ("GDPR"), the California Consumer Privacy Act AB-375 ("CCPA") and the Biometric Information Privacy Act 740 ILCS 14 ("BIPA").

FHE is a relatively new and emerging cryptography field that operates on encrypted data without decryption and supports applications where the input data, output data and the occurrence of search itself must be concealed.[1,]

Traditional biometric recognition systems involve the use and storage of plaintext biometrics through which a template or image with the features extracted from an original biometric is stored and used during subsequent authentication attempts. This storage or use of plaintext biometrics presents data privacy risks. Even where the data is stored in a decentralized fashion or divided form, it must be decrypted to plaintext to support the match operation and thus is covered by privacy laws.

Until recently, FHE cryptosystems were not practical or scalable for business applications.[2] In late 2018, however, Microsoft launched SEAL, a set of open source, state-of-the-art homomorphic encryption libraries. Google then followed in 2019 with the release of its open-source homomorphic cryptography tool.[3] A handful of additional companies are now producing commercial FHE systems including IBM®, Enveil®, Duality Technologies and Private Identity.

Based on Private Identity's description of the technology and our review of the technical documents provided, we understand that the Cloud Biometric MFA system works as follows.

a. An individual/end user accesses the Cloud Biometric MFA system, which then grants the end-user a license to run an application on his or her device (e.g. a phone or web browser) to acquire his/her own biometric data (face, voice or fingerprint). This

---

[1] Lyu, Lingjuan et al. "Towards Fair and Privacy-Preserving Federated Deep Models." IEEE Transactions on Parallel and Distributed Systems 31 (2020): 2524-2541.

[2] Chirgwin, R. "IBM's homomorphic encryption accelerated to run 75 times faster." (2018) Retrieved from The Register: https://www.theregister.com/2018/03/08/ibm_faster_homomorphic_encryption

[3] Labrozzi, Greg. *Homomorphic Encryption: Outsourcing and Sharing Healthcare Data in Public Clouds*. Diss. Utica College, 2020. Walker, Amanda, Sarvar Patel and Moti Yung. "Helping organizations do more without collecting more data." Google Security Blog. June 19, 2019. Retrieved 7/27/2020 https://security.googleblog.com/2019/06/helping-organizations-do-more-without-collecting-more-data.html

application only operates on the local device. Private Identity cannot view, access or otherwise process the plaintext biometric data on the local device.[4,]

b. This application then transforms the biometric data using a one-way cryptographic hash function into irreversibly anonymous FHE payloads that are globally unique (i.e. no two payloads are ever the same), positional arrays of 128 floating-point numbers that do not contain biological or behavioral characteristics, imagery or a template of any physiological, biological or behavioral trait (the "FHE payloads").

c. This FHE payload is the only data transmitted to Private Identification. No third party can view the plaintext biometric. Private Identity only uses the FHE payload to perform its match and search operations. The FHE payload is not a biometric template.[5]

d. Private Identity does not receive or store any personal data about the individual/end user. Instead of using a username or email address, the Cloud Biometric MFA system labels each end user with a randomly generated, customer-specific universally unique identifier ("UUID") that cannot be tied back to an individual/end user by Private Identity. The system collects no name, machine or device identification number, metadata, or any other personal data during the exchange or otherwise.

Accordingly, the Private Identity FHE system irreversibly anonymizes personal data. This creates secure access without holding or storing any personal data.

We next consider the GDPR, the CCPA and the BIPA and discuss the extent to which those laws apply to the FHE payloads and UUID processed by the Cloud Biometric MFA system. [6]

---

[4] An organization enrolling, matching or searching biometrics on a larger scale (i.e. more than one end user at a time) will start by downloading and installing the Cloud Biometric MFA system's "Encryption Engine" that runs on the organization's infrastructure and contains the same FHE transformation service described above.

[5] Traditional biometric recognition systems involve the use and storage of plain text biometrics through which a template or picture with the features extracted from an original biometric is stored and used during subsequent authentication attempts to match features. The storage or use of plain text biometrics presents data privacy risks through loss of the biometric information. Even where the data is stored in a decentralized fashion or divided form, it must be decrypted to match for authentication purposes and thus has inherent privacy risks and are covered by several privacy laws.

[6] Private Identity's solution will generally be deployed within an overall data gathering architecture that includes consent and notice to process anonymized UUIDs and encrypted FHE payloads. An important goal of data privacy laws is ensuring transparency in the collection, use, retention, and sharing of personal data. To the fullest extent possible, every organization is encouraged to implement processes and consumer notices that meet that goal. Private Identity, on a voluntary basis, informs end users of its process and seeks acknowledgment that end users understand and agree to its use of anonymized UUIDs and encrypted hashed data. This voluntary consent process is for transparency and not legally mandated given that personal data is not collected, transmitted, or stored. To the extent that the UUID held by a Private Identity customer is combined with other personally identifiable data

Please note this memorandum contains the professional views of the authors, based on the information received and on regulatory guidance currently available on the key principles under the relevant laws discussed. This is not a formal legal opinion letter. There can be no assurance that our views will be adopted by UK, EU or US courts or regulators. Private Identity customers should seek their own independent legal advice.

3. GDPR ANALYSIS

The GDPR was adopted by the European Union in April 2016, with a key aim of making it easier for EU citizens to understand how their data is being used and to exert additional control over such data usage. The GDPR was adopted, amongst other things, following growing concerns about the misuse of sensitive personal data (i.e. a lack of transparency around how data was being used by organisations) and the absence of effective legal remedies where organisations were deemed to have used personal data unlawfully.

The GDPR contains the six data protection principles set out below. Organizations are "accountable" to demonstrate compliance with these principles when processing "personal data."

Where the GDPR applies, the data protection principles provide that personal data must be:

a. processed lawfully, fairly and in a transparent manner in relation to the data subject (i.e. the lawfulness, fairness and transparency principle);

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (i.e. the purpose limitation principle);

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (i.e. the data minimization principle);

d. accurate and, where necessary, kept up to date (i.e. the accuracy principle);

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (i.e. the storage limitation principle); and

also held by the customer, the UUID outside of the Cloud Biometric MFA system may potentially be treated as an identifier covered by data privacy laws when in the hands of the customer. However, Private Identity does not have anything in its possession which it could link to the UUID such that the UUID would become personal data (and has no lawful way to seek to link the UUID to an individual).

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (i.e. the integrity and confidentiality principle).[7]

These principles must lie at the heart of each organization's approach to processing personal data.

The Cloud Biometric MFA system enables customers to advance the principles of the GDPR by transforming biometrics into anonymized FHE payloads. This eliminates the requirement for organizations to gather personal data to support robust security and advances the integrity and confidentiality principle and the data minimization principle of the GDPR.[8] Please see chart at Appendix A to view in greater detail how the Cloud Biometric MFA system seeks to enable customers to advance each of these principles.

3.1. FHE Payloads Contain Anonymized Data

The GDPR provides a high bar for achieving data anonymization. This process is described in the GDPR Recital 26:

> *"To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.*
>
> *To ascertain 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".*

To be classified as anonymized data, the deidentification of the personal data must be "irreversible" and must be retained in a form in which identification of a data subject "is no longer possible."[9,10]

[7] Art. 5 GDPR Principles relating to processing of personal data.

[8] GDPR Article 5(1)(c)

[9] Recital 26 of the GDPR.

[10] Opinion 05/2014 on anonymisation techniques, 10 April 2014.

Turning to the FHE payloads and UUIDs, we consider whether these are anonymized data by applying the following criteria:

- Do the FHE payloads or UUIDs contain any identifiers or other data that could identify the individual or device to whom the data relates?
- Is there any data in Private Identity's possession that could be combined with the FHE payloads or UUIDs to identify the individual or device to whom the data relates?
- Are the FHE payloads or UUIDs reversible?
- Can the FHE payloads or UUIDs be linked to an individual?

The answer is "no" to each for reasons set out above. Thus, we find that the FHE payloads and UUIDs are not personal data under the GDPR. Accordingly, the GDPR's principles do not apply to the FHE payloads or UUIDs.

3.2. FHE Payloads Do Not Contain Biometric Data

We next consider biometric data. Biometric data is required to be treated as a special category of personal data under the GDPR and is subject to increased compliance obligations.[11] The GDPR defines biometric data as:

> *"personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data".*[12]

We find that the FHE payload and UUID do not qualify as biometric data. In particular, the FHE payload is a globally unique, positional array of 128 floating-point numbers that does not contain biological or behavioral characteristics, imagery or a template of any physiological, biological or behavioral trait.

The UUID is a randomly generated, universally unique identifier that cannot be tied back to an individual/end user once assigned and in the possession of Private Identity.

[11] GDPR Article 9, Recital 51.
[12] GDPR Article 4(14).

3.3. FHE Payloads Are Not Subject to GDPR Obligations

The GDPR does not regulate the processing of anonymized information.[13] In Recital 26, the GDPR specifically refers to anonymization to exclude anonymized data from the scope of the data protection legislation, stating:

> *"The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes".*[14]

We conclude that the FHE payloads and UUIDs are not subject to the requirements of GDPR because they constitute anonymized data and do not contain personal data or biometric data.

4. CCPA ANALYSIS

The CCPA (California Civil Code §§ 1798.100 to 1798.199) is currently the most comprehensive privacy legislation in the United States. The CCPA is similar to the GDPR in that it grants California residents robust data privacy rights and control over their personal information, including a subset of the elements of the GDPR's lawfulness, fairness and transparency principle, data minimization principle, and integrity and confidentiality (security) principle.

The CCPA grants California residents rights with respect to the collection of their personal information, including the right to be forgotten (deletion of information), the right to opt-out of the sale of their personal information, and the right to know what information a business collects about them. The Cloud Biometric MFA system advances the individual rights of California residents with respect to: (a) the collection of their personal information by transmitting, storing and using only deidentified data, and (b) providing strong end-user authentication that allows businesses to accurately identify each data subject without requiring the subject to remember a username, password, token or shared secret.

The CCPA's broad definition of personal information includes any plaintext data or pseudonymized data that remains capable of being associated with a particular consumer or household. The CCPA does not restrict a business's ability to collect, use, retain, sell, or disclose consumer information that is "deidentified" (anonymized). The Cloud Biometric MFA system helps advance the CCPA's data minimization goals by transmitting, storing and using

[13] GDPR Recital 26.
[14] GDPR Recital 26.

(processing) only deidentified data and deleting all personal information immediately after it is transformed into FHE payloads.

The CCPA maintains that a business has, *"[a] duty to implement and maintain reasonable security procedures and practices."* This security provision includes a proportionality element providing that it is the duty of the business to maintain reasonable security procedures and practices, *"appropriate to the nature of the information."* The Cloud Biometric MFA system aids a business in advancing this goal and responding to requests from subjects seeking to exercise their rights under the CCPA by providing strong end-user authentication that allows organizations to accurately identify each data subject without requiring the subject to remember a username, password, token or shared secret.

4.1. FHE Payloads Contain Deidentified Information

The CCPA defines and regulates "personal information" as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[15] The Cloud Biometric MFA system fully realizes the CCPA's legislative goals by transforming personal information into FHE payloads and UUIDs that are treated as "deidentified" data under the CCPA.

As discussed in detail above, the Cloud Biometric MFA system only transmits, stores or uses deidentified (anonymized) data. Additionally, the Cloud Biometric MFA system does not transmit, store or use any other personal data or biometric data, machine or device identifications, metadata, or any other identifying information.

4.2. FHE Payloads Do Not Contain Biometric Information

The CCPA defines biometric information as follows.

> *"…an individual's physiological, biological or behavioral characteristics, including an individual's DNA, that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information."*[16]

We find, under the plain language of this section, the encrypted FHE payloads and UUIDs created by Cloud Biometric MFA system do not qualify as biometric data under the CCPA.

[15] CCPA 1798.140(o)(1).
[16] CCPA 1798.140(b).

These FHE payloads and UUIDs contain no biological or behavioral characteristics, imagery or a template of any physiological, biological or behavioral trait.

Accordingly, the encrypted FHE payloads and UUIDs should not be treated as biometric information under the CCPA.

4.3. FHE Payloads Are Not Subject to CCPA Obligations

The CCPA states that businesses processing deidentified data are not obligated to provide or delete information in response to a consumer request or to re-identify individual data to verify a consumer request. Specifically, the final text of the California Consumer Privacy Act Regulations at § 999.323(f) provides that, *"If a business maintains consumer information that is deidentified, a business is not obligated to provide or delete this information in response to a consumer request or to re-identify individual data to verify a consumer request."*

In addition, the CCPA Regulations at § 1798.140 further excludes deidentified information from the scope of the legislation.

> *""Deidentification" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly to a particular consumer, provided that a business that uses deidentified information [has implemented technical and process safeguards that prohibit reidentification of the consumer, has implemented processes to prevent inadvertent release of deidentified information, and makes no attempt to reidentify the information."*[17]

Finally, in the same section, CCPA § 1798.145(a)(5) further provides that nothing in the CCPA restricts a business's ability to *"collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate."*[18]

As previously described, the FHE payloads and UUIDs contain only deidentified data. Therefore, the consumer rights provided under the CCPA thus fall away with respect to this deidentified information and businesses that utilize this system do not incur CCPA obligations.

5. BIPA ANALYSIS

BIPA (740 ILCS 14) is the most stringent biometric privacy law in the U.S. It requires covered businesses to inform consumers in writing that biometric identifiers or biometric information is collected and stored, of the purpose and length of time of biometric information storage and use, and to secure written consent from consumers. BIPA also prohibits covered businesses from profiting from biometric data, permits only a limited right to disclose the data, mandates

[17] CCPA 1798.140(h).

[18] CCPA § 1798.145(a)(5). Underline added for emphasis.

protection obligations and retention guidelines, and creates a private right of action for any individuals harmed by violators of BIPA.

BIPA applies to both biometric identifiers and biometric information. Under BIPA, a "biometric identifier" includes specific types of information including fingerprint, voiceprint, retina/iris scan, scans or records of hand or face geometry.[19] Biometric information includes *"any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual."*[20] Illinois courts have specifically found that face-scan measurements (i.e. a biometric template) derived from user-uploaded photos qualify as "biometric information" under BIPA.[21]

BIPA grants residents of Illinois rights with respect to the collection of their biometric identifiers or biometric data. Under BIPA, notices require private entities to inform consumers that: (1) biometric identifier or biometric information is being collected and stored; and (2) *"[the] specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used."* In addition, BIPA requires affirmative consent for virtually any data collection in all circumstances for both commercial and non-commercial purposes.

5.1. FHE Payloads Do Not Contain Biometric Identifiers or Biometric Information

Biometric identifiers and biometric information under the BIPA are subject to increased compliance obligations. The biometric identifier under the BIPA includes specific types of information including fingerprint, voiceprint, retina/iris scan, scans or records of hand or face geometry.[22] And, the biometric information under the BIPA includes, "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." Illinois courts have further stated in *Rivera v. Google, Inc.* that face-scan measurements (i.e. a biometric template[23]) derived from user-uploaded photos qualify as "biometric information" under BIPA.[24]

As discussed above in Section 3.1 and 4.1, the Cloud Biometric MFA system advances the rights of Illinois residents with respect to the collection of their biometric identifiers or biometric

[19] 740 ILCS 14/10.

[20] 740 ILCS 14/10.

[21] *Rivera v. Google, Inc*., 238 F. Supp. 3d 1088 (N.D. Ill. 2017).

[22] 740 ILCS 14/10.

[23] Traditional biometric recognition systems involve the use and storage of plaintext biometrics through which a template or image with the features extracted from an original biometric is stored and used during subsequent authentication attempts to match features. The storage or use of plaintext biometrics presents data privacy risks through risk of loss of the biometric information. Even where the data is stored in a decentralized fashion or divided form, it must be decrypted to plaintext to support the match operation and thus has inherent privacy risks and are covered by several privacy laws.

[24] *Rivera v. Google, Inc*., 238 F. Supp. 3d 1088 (N.D. Ill. 2017).

information by only transmitting, storing or using anonymized data. To accomplish this, the system grants each end user a license to run application software on the user's local device. Using this application, the user collects his/her own biometric data. This data is then transformed (encrypted) by a one-way cryptographic hash function on the local device and becomes FHE payloads. FHE payloads are globally unique positional arrays of 128 floating-point numbers that do not contain biological or behavioral characteristics, imagery or a template of any physiological, biological or behavioral traits.

Accordingly, we find the Private Identity MFA system only transmits, stores or uses deidentified data and no biometric identifiers or biometric information. Under the plain language of this section and the Illinois state court interpretation, we find the encrypted FHE payload should not be treated as biometric identifiers or biometric information.

5.2. FHE Payloads Do Not Incur BIPA Obligations

The BIPA obligations apply only to biometric information. As discussed immediately above in Section 5.1, we find the Cloud Biometric MFA system does not contain biometric information or biometric identifiers.

Accordingly, an organization using the Cloud Biometric MFA system is not collecting or storing biometric information and, with respect to this system, eliminates the requirement to comply with BIPA obligations including the consent requirements and the requirement for an organization to protect and store biometric data at least to the same degree it protects other confidential or sensitive information.[25]

[25] BIPA (740 ILCS 14/15(e)(2))

EXHIBIT A

	KEY GDPR PRINCIPLES	CLOUD BIOMETRIC MFA SYSTEM
1	**Lawfulness, fairness and transparency principle**	**Processes only anonymized data** The Cloud Biometric MFA system processes only anonymized data. This reduces the risk of the biometric data being used for any improper, concealed or illegal purpose. **Provides strong end-user authentication.** The GDPR requires the organization to take reasonable steps to confirm that the person requesting access to their personal data is actually the rightful data subject.[26] The Cloud Biometric MFA system helps organizations advance and respond to requests from data subjects to exercise their rights under data protection law by providing strong end-user authentication to enable each data subject to control one's data, to no longer consent to processing, to correct significant errors within the data and to request that data be erased (forgotten). Strong end user authentication also allows organizations to accurately identify each data subject without requiring the subject to remember a username, password, token or shared secret.
2	**Purpose limitation principle**	**Processes only anonymized data** The Cloud Biometric MFA system transmits, stores and uses only anonymized data. As such, no personal data is being used in a way which breaches this principle.
3	**Data minimization principle**	**Processes only anonymized data** The Cloud Biometric MFA system transmits, stores and uses only anonymized data. This promotes and accomplishes the regulatory goal of limiting the processing of personal data to only what is necessary. **Discards (deletes) all personal data** The Cloud Biometric MFA systems discards all personal data and biometric data. Only anonymized data is transmitted, stored or used to support the enrollment and authentication process. This helps realize the regulatory goal of limiting the processing of personal data to only what is necessary.

[26] Recitals 65 and 66 and in Article 17 of the GDPR.

4	**Accuracy principle**	**Processes no personal data** The GDPR requires organizations to ensure that personal data are kept accurate and up to date. The regulation further states that personal data that are inaccurate must be deleted or rectified without delay. Since no personal data is being processed, this principle is not breached. The Cloud Biometric MFA system only transmits, stores, and uses the anonymized data necessary for the authentication process.
5	**Storage limitation principle**	**Processes only anonymized data** The Cloud Biometric MFA system transmits, stores and uses only anonymized data and deletes the biometric data on the end user's local device immediately after the FHE transformation. This promotes and accomplishes the regulatory goal of storing personal data for no longer than is necessary.
6	**Integrity and confidentiality principle (security)**	**Provides strong end-user authentication** Strong end-user authentication is a key part of the security framework anticipated by the GDPR. In addition, Strong Customer Authentication (SCA) is required by PSD2 for "customer-initiated" online payments within Europe.[27] The Cloud Biometric MFA system provides strong end-user authentication to help organizations secure personal data.[28] This allows organizations to accurately identify each data subject without requiring the subject to remember a username, password, token or shared secret.

[27] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication. [Link]

[28] Recitals 65 and 66 and in Article 17 of the GDPR.