LOVE & NORRIS
Attorneys at Law

March 8, 2023
Georgia McKnight
Memo Re: Data Erasure and GDPR

In May of 2018, the European Union passed the General Data Protection Regulation ("GDPR"), the toughest privacy and security law in the world to date.[1] In the age of the Internet and other quickly evolving technologies, this regulation seeks to protect individuals by requiring organizations to safeguard personal data and uphold the privacy rights of anyone in EU territory.

Despite this admirable goal, the GDPR without its accompanying exemptions poses serious risk to child protection efforts. Were the regulation to require the removal of applicant records, the GDPR would expose organizations serving children to liability in child sexual abuse matters. Although such regulation has not been emulated in the U.S., lawmakers need to be aware of these ramifications to child-serving organizations. If equivalent legislation is passed stateside, it is necessary to include the current GDPR exemptions as well as carve out additional exceptions for child-serving organizations.

History and Application of the GDPR
As written, the GDPR creates an individual's right to data erasure, also known as the "right to be forgotten."[2] Lawmakers ascribe the origin of this right to the 1950 European Convention on Human Rights which states, "Everyone has the right to respect for his private and family life, his home and his correspondence."[3] Following the rapid advance of technology since then, GDPR legislation was enacted as the modern protection of this *private life*.

In application, the right to be forgotten requires organizations to erase personal data in the event of several scenarios:

- The personal data[4] is no longer necessary for the purpose an organization originally collected or processed it.
- An organization is relying on an individual's consent as the lawful basis for processing the data and that individual withdraws their consent.

[1] *See* https://gdpr.eu/what-is-gdpr/
[2] The full text of Article 17 is provided at the end of this memorandum.
[3] European Convention on Human Rights, Article 8.
[4] The GDPR defines "personal data" as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." Article 4, Section 1.

- An organization is relying on legitimate interests as its justification for processing[5] an individual's data, the individual objects to this processing, and there is no overriding legitimate interest for the organization to continue with the processing. An organization is processing personal data for direct marketing purposes and the individual objects to this processing.
- An organization processed an individual's personal data unlawfully.
- An organization must erase personal data in order to comply with a legal ruling or obligation.
- An organization has processed a child's personal data to offer their information society services.[6]

On the other hand, however, an organization may decline to erase an individual's data for any of the following reasons ("exemptions"):

- The data is being used to exercise the right of freedom of expression and information.
- The data is being used to comply with a legal ruling or obligation.
- The data is being used to perform a task that is being carried out in the public interest or when exercising an organization's official authority.
- The data being processed is necessary for public health purposes and serves in the public interest.
- The data being processed is necessary to perform preventative or occupational medicine. This only applies when the data is being processed by a health professional who is subject to a legal obligation of professional secrecy.
- The data represents important information that serves the public interest, scientific research, historical research, or statistical purposes and where erasure of the data would likely to impair or halt progress towards the achievement that was the goal of the processing.
- The data is being used for the establishment of a legal defense or in the exercise of other legal claims.[7]

Therefore, the right to be forgotten is not an absolute one. Rather, when considering requests for data erasure, a data controller is required to compare the subjects' rights to "the public interest in the availability of the data."[8]

In most cases, this ability to control personal data is a positive phenomenon. Indeed, under the GDPR individuals are not left helpless if their personal information is misused, shared, or resold to a third party. Because this is often a reality in our increasingly data-driven world, data protection is a valuable right. Despite the benefits of data erasure, however, legislators must also be aware of the potential impact on child safety efforts.

---

[5] The GDPR defines "processing" as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

[6] *See* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulationgdpr/exemptions/.

[7] *See* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulationgdpr/exemptions/.

[8] The General Data Protection Regulation, 3 Records Retention § 68:3.75.

Impact on Child Protection Efforts

Today, the collection of data dominates the employment process and child-protection recordkeeping. This information-gathering stage, also called screening, is the method by which an employer examines each applicant using a variety of tools: applications, reference checks, interviews and criminal background checks.[9] By considering records of past performance and behavior, employers are able to make more informed decisions about a candidate's suitability for employment and potential risk.

For child-serving organizations, screening is not only a wise business practice, but also constitutes a standard of care, often required to secure insurance coverage and satisfy licensure requirements.[10] To meet this standard of care, an organization must show that it took reasonable steps to mitigate the known risk of child sexual abuse. Upon completion of screening, employers keep records of the applicants they intend to hire (or not hire), evidencing the proper steps taken to comply with standards of care and avoid future liability.

With the advent of data erasure rights, records kept in accordance with standards of care must be safeguarded. Under the GDPR as written, several exemptions would likely apply to a child-serving organization requested to remove personal data. These would include exemptions pertaining to furtherance of public interest as well as that referencing data "used to comply with a legal ruling or obligation." Without these safe harbors, however, organizations serving children would be required by law to expose themselves to potential liability for child sexual abuse, as well as depart from insurance carrier requirements. Clearly, these competing interests cannot coexist. In any U.S. iteration of data protection, legislators must be aware of the risks and ramifications to child-serving organizations – promotion of the individual's rights privacy over the reasonable efforts of organizations to manage risk.

Scope of the GDPR

At present, the GDPR's impact on child protection is predominantly limited to the EU.[11] However, pursuant to Article 3.2 the territorial scope of the law extends to data processers outside the EU if two conditions are met: the organization offers goods or services to people in the EU, or the organization monitors the online behavior of people in EU.

Moreover, a trend of similar legislation has emerged in the US. For instance, California passed the California Consumer Privacy Act ("CCPA") in 2020, which gives Californian residents greater transparency and control over how businesses collect and use their personal information.[12] This is essentially the US equivalent to the GDPR. Similarly, Virginia enacted a comprehensive data protection law, the Consumer Data Protection Act ("CDPA"), which went into effect on January 1, 2023.[13] Several other states, including Colorado, Utah and Connecticut, have passed similar privacy laws that will go into effect over the course of 2023.

---

[9] *See* Ann Marie Ryan & Maria Lasek, *Negligent Hiring and Defamation; Areas of Liability Related to Pre-Employment Inquiries*, 44 PERSONNEL PSYCHOL 293, 304 (1991).

[10] Maria Mossaides and Suzin Bartley, *Guidelines and Tools for the Development of Child Sexual Abuse Prevention and Intervention Plans by Youth-Serving Organizations in Massachusetts*, The Massachusetts Legislative Task Force on Child Sexual Abuse Prevention, 33 (2017).

[11] The full text of Article 3 is included at the end of the memorandum.

[12] *See* https://oag.ca.gov/privacy/ccpa

[13] The CDPA closely follows the framework of the CCPA; however, there are a few key differences:

Summary
As support gathers for further data protection regulation, U.S. lawmakers must be aware of all interests at play. As written, the GDPR carefully curtails the right to be forgotten with exemptions promoting public interest. If similar data erasure rights are considered in the U.S., it is necessary to include current exemptions found in the GDPR, as well as carve out other data protection exceptions for child-serving organizations.

APPENDIX – General Data Protection Regulation

Art. 3 GDPR

• The CDPA contains no private right of action. Rather, all actions must be brought by the Virginia Attorney General.
• The CDPA, like the CCPA, exempts data that is already regulated by certain listed federal laws, such as HIPAA, GLBA, FCRA, FERPA and COPPA. However, under the CDPA, the GLBA exemption is broader as it wholly exempts financial institutions, not just data subjects. Additionally, there are data-based exemptions for the Fair Credit Reporting Act, the Driver's Privacy Protection Act, and the Federal Education Rights and Privacy Act, and nonprofit organizations.
• The CDPA contains an opt-in requirement to process sensitive personal data, unless exempted.
• The CDPA defines "consumer" more narrowly than the CCPA. The CDPA excludes those acting in a commercial or employment context.
• Under the CDPA, the "sale of personal information" requires that the consideration be monetary to qualify as a sale of data. On the contrary, the CCPA allows monetary or "other valuable consideration."
https://www.natlawreview.com/article/gdpr-usa-new-state-legislation-making-closer-to-reality

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

    a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

    b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Art. 17 GDPR

Right to erasure (‘right to be forgotten’)

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

    a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

    b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

    c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

    d) the personal data have been unlawfully processed;

    e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

a) for exercising the right of freedom of expression and information;

b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

e) for the establishment, exercise or defence of legal claims.