Freshfields Bruckhaus Deringer

When Less is More: Making the Business Case for Data Minimization
Privacy + Security Forum, November 2023

1. **Examples of Data Minimization Standards Under Data Protection Laws**

   (a) **GDPR**: "Personal data shall be…adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')." (Art. 5(c))

   (b) **Virginia Consumer Data Privacy Act**: "A controller shall…limit the collection of personal data to what is relevant, adequate, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer." (Code of Virginia §59.1-578(A))

   (c) **Colorado Privacy Act:** "A controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes for which the data are processed." (Colorado Revised Statutes §6-1-1308(3))

   (d) **California Consumer Privacy Act**: "A business' collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes." (Cal. Civ. Code §1798.100(c))

2. **Fundamental Elements of Data Minimization**

   (a) ***Adequate***: sufficient to properly fulfill your stated purpose

      (i) In this respect, data minimization is necessarily about collecting the absolute minimum amount of PI—it's qualitative as well as quantitative.

      (ii) ICO guidance on data minimization: "In some circumstances you may need to collect more personal data than you had originally anticipated using, so that you have enough information for the purpose in question."

   (b) ***Relevant***: reasonably related to the stated purpose

      (i) May be necessary to consider relevance separately by individual or category of individual, rather than collecting/processing the same types of PI across all individuals in a group

      (ii) ICO guidance on data minimization: "**Example:** A recruitment agency places workers in a variety of jobs. It sends applicants a general questionnaire, which includes specific questions about health conditions that are only relevant to particular manual occupations. It would be irrelevant and excessive to obtain such information from an individual who was applying for an office job."

   (c) ***Limited to what is reasonably necessary***: not collecting or retaining more than needed for that purpose

(i) For example, not collecting personal information beyond what is currently needed just because it might turn out to be useful in the future

(A) Irish DPC guidance on data minimization: The data minimization principle "essentially means that data controllers should **collect the minimum amount of data they require** for their **intended processing operation**; they should never collect unnecessary personal data. This principle complements, in particular, the principle of purpose limitation, but also supports compliance with the range of data protection principles."

(B) ICO guidance on data minimization: "**Example:** An employer holds details of the blood groups of some of its employees. These employees do hazardous work and the information is needed in case of accident. The employer has in place safety procedures to help prevent accidents so it may be that this data is never needed, but it still needs to hold this information in case of emergency.

If the employer holds the blood groups of the rest of the workforce, though, such information is likely to be irrelevant and excessive as they do not engage in the same hazardous work."

(ii) Retaining the personal information only as long as needed for the specified purpose, rather than retaining the information indefinitely

(A) For example, the Irish DPC guidance on data minimization highlights the role of storage limitation in data minimization:

(I) **"Data Minimisation**: Processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum (see also the principle of 'Storage Limitation'…)."

(B) General requirement to delete personal data when it is no longer needed

(I) From Irish DPC guidance on storage limitation: **"**Controllers must hold personal data, in a form which permits the identification of individuals, **for no longer than is necessary for the purposes** for which the personal data are processed….Controllers should therefore, in general, **delete personal data as soon as it ceases to be necessary for the purposes for which it was originally collected**. To this end, the GDPR recommends that time limits should be established by the controller for erasure or for a periodic review."

(C) Anonymization as a potential alternative to deletion

(I) From ICO guidance on storage limitation: "What should we do with personal data that we no longer need? You can either erase (delete) it, or anonymise it."

(II) Anonymization is a high standard and requires measures to prevent reidentification or linking of new data

(aa) Per EDPB Opinion 05/2014 on Anonymisation Techniques: "An effective anonymisation solution prevents all parties from singling out an individual in a dataset, from linking two records within a dataset (or between two separate datasets) and from inferring any information in such dataset. Generally speaking, therefore, removing directly identifying elements in itself is not enough to ensure that identification of the data subject is no longer possible. It will often be necessary to take additional measures to prevent identification…" (p. 9)

(bb) From Irish DPC guidance on storage limitation: "Data are truly anonymous, and therefore no longer 'personal' data, only if the individual is no longer identifiable; however, if data could still be attributed to an individual by the use of additional information it would be only 'pseudonymised' and thus still considered personal data. If the process applied to supposedly anonymise personal data is not permanent and can be reversed, then the data has not been anonymised."

(cc) From Spain's data protection authority (AEPD): "[A]nonymisation procedures must ensure that not even the data controller is capable of re-identifying the data holders in an anonymised file."

(dd) See FTC guidance on sensitive data: "Firms making claims about anonymization should be on guard that these claims can be a deceptive trade practice and violate the FTC Act when untrue. Significant research has shown that "anonymized" data can often be re-identified, especially in the context of location data."

(III) Differing exceptions by law

(aa) CCPA exceptions for "de-identified data" and "aggregate consumer information," which no longer need to be treated as personal information (Cal. Civ. Code 1798.140(v)(1)(3)

(bb) Under CCPA, "deidentified" means "information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer provided that the business that possesses the information:

(1) Takes reasonable measures to ensure that the information cannot be associated with a consumer or household.

(2) Publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision.

(3) Contractually obligates any recipients of the information to comply with all provisions of this subdivision." (Cal. Civ. Code 1798.140(m))

(cc) Under CCPA, "aggregate consumer information" means "information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified." (Cal. Civ. Code 1798.140(b))

(D) Pseudonymization can be a helpful data minimization tool—but remember that pseudonymized data (unlike anonymized data) remains personal data

(I) Under GDPR, pseudonymization has value as a data minimization technique for personal data

(aa) "[T]he controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, **such as pseudonymisation**, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects." (GDPR Art. 25, emphasis added)

(bb) Under GDPR, 'pseudonymisation' means "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." (GDPR Art. 4(5))

(II) Similarly, CCPA treats pseudonymization as a safeguard (specifically, for research activities—see Cal. Civ. Code 1798.140(ab)), but does not exclude pseudonymized data from the scope of personal information covered by the law

3. **Resources**

(a) UK Information Commissioner's Office (ICO) guidance on data minimization: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/data-minimisation/

(i) ICO guidance on storage limitation: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/storage-limitation/

(b) Irish Data Protection Commissioner, Quick Guide to the Principles of Data Protection: https://www.dataprotection.ie/sites/default/files/uploads/2019-11/Guidance%20on%20the%20Principles%20of%20Data%20Protection_Oct19.pdf

(c) EDPB Opinion 05/2014 on Anonymisation Techniques: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

(d) UK draft updated guidance on anonymization, pseudonymization, and privacy enhancing technologies: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-call-for-views-anonymisation-pseudonymisation-and-privacy-enhancing-technologies-guidance/

(i) See also Freshfields' analysis, "Thinking of adopting a PET? ICO issues draft guidance on privacy enhancing technologies" by Adam Gillert and Taybah Siddiqi