

The Data Privacy Chronicle

Edition # 4 - Less is more: rediscovering data minimization

The Data Privacy Chronicle is a sequence of pragmatic newsletters mainly designed for Data Protection Officer (“DPOs”), privacy leaders and their respective organisations. The aim is simple: to provide you with practical insights, powered by our experience as data protection lawyers and DPO-as-a-Service providers, on emerging topics that shape your role and to help you navigate the growing complexity of regulatory frameworks in the digital era.

This edition focuses on a topic that is often underestimated in practice, despite its central role in effective data governance: **data minimization**.

1. Introduction: the culture of “just in case” data collection

In practice, many organisations tend to retain more personal data than strictly necessary. Information is often collected and stored, whether on paper or electronically, on the assumption that it may prove useful at a later stage. The increasing availability of storage and the growing importance of data in business operations have reinforced this tendency.

However, this mindset does not align with one of the core principles of European data protection law: **data minimization**. Under the General Data Protection Regulation (“**GDPR**”), organisations must ensure that personal data are adequate, relevant and limited to what is necessary for the purposes for which they are processed.

Although the principle appears relatively clear, its practical application often raises complex questions. Determining what data can be considered “necessary” depends on the specific purposes of the processing, the operational context and, in some cases, applicable regulatory obligations.

For companies operating in a highly regulated and data-driven environment (such as Luxembourg), these questions are particularly relevant. As in the rest of the European Union, organisations are expected to ensure that personal data processing remains necessary and proportionate to the purposes pursued.

The supervisory authority, the *Commission nationale pour la protection des données* (“**CNPD**”), oversees the application of the GDPR and the compliance with this requirement.

2. The data minimization principle: what does it really require?

The principle of data minimization is set out in Article 5(1)(c) of the GDPR. It requires that personal data be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

At first glance, the principle seems relatively simple, organisations should not collect or retain personal data that they do not need. In practice, however, determining what is “necessary” is rarely straightforward. The main challenge is deciding what “necessary” actually means in a given situation. This requires organisations to clearly define the purpose of the processing and to assess what data is genuinely required to achieve it.

In this context, it is not enough to ask whether data may be useful. Organisations should also consider whether the same objective could be achieved with less data, less detailed information, or even without processing personal data at all, as highlighted in the [Guidelines 4/2019 of the European Data Protection Board](#).

Data minimization is also not limited to the point of collection. It applies throughout the lifecycle of personal data, from collection and use to access, storage and eventual deletion or anonymisation. As noted by the European Data Protection Board, this may include reducing the level of identification, for example through pseudonymisation or anonymisation once direct identification is no longer required.

This approach requires organisations to take data minimization, along with other data protection considerations, into account when designing their systems and processes from the outset.

As a result, applying the data minimization principle often requires organisations to review their data collection practices and internal processes in a structured way. Such reviews frequently reveal that significantly more personal data is collected or retained than is strictly necessary for the intended purposes.

3. Data minimization in context: not an isolated principle

Although data minimization is often discussed as a standalone requirement, in practice it must be applied in conjunction with the other principles governing the processing of personal data under the GDPR.

In particular, it should be considered in light of the principles of data protection by design and by default, which require organisations to take data protection into account when designing their processing activities from the outset.

Data minimization is also closely linked to purpose limitation. Personal data should only be collected for specified and legitimate purposes, which in turn helps determine what data can reasonably be considered necessary.

Data minimization is also connected to the principle of storage limitation, which requires organisations to retain personal data only for as long as necessary for the relevant purposes. Even where the initial collection of data may be justified, retaining it indefinitely would conflict with this requirement. In addition, minimization plays a key role in ensuring integrity and confidentiality. The more personal data an organisation stores, the greater the potential exposure in the event of unauthorised access, loss or misuse.

Finally, the principle must be understood in light of the broader concept of accountability. Organisations are expected not only to comply with these principles, but also to be able to demonstrate that their data processing practices reflect them in practice.

Taken together, these principles illustrate that data minimization should not be treated as an isolated compliance requirement. Rather, it forms part of a broader framework aimed at ensuring that personal data processing remains proportionate, justified and properly governed.

In practice, applying these principles consistently can be particularly challenging in certain sectors.

4. A cross-sector challenge: where data minimization becomes particularly complex.

While the principle of data minimization applies to all organisations processing personal data, its practical implementation often becomes more complex in sectors where large volumes of information are processed or where regulatory requirements impose specific data collection or retention obligations.

In these contexts, organisations must balance operational needs, sector-specific regulations, business practices and data protection requirements.

a. Financial sector

Luxembourg's financial sector provides a clear example of the challenges associated with data minimization. Financial institutions must collect and retain significant amounts of personal data in order to comply with regulatory requirements, particularly in the context of client identification and anti-money laundering (AML) obligations.

However, in practice, data minimization issues often arise not from regulatory requirements themselves, but from the way data is collected, shared and retained across different internal systems.

For example, during client onboarding, institutions frequently collect a wide range of information about clients and beneficial owners through standardised onboarding forms and documentation requirements. While many of these elements are necessary to comply with regulatory obligations, in practice onboarding processes may also include additional data fields that are not strictly required for the specific risk assessment being carried out.

The situation may arise, for example, where onboarding templates have been expanded over time or where the same forms are used across different types of clients or services. In such cases, institutions should periodically review whether all requested information remains relevant and necessary for the specific compliance or business purpose.

b. Human resources and employee data

Human resources processes also frequently raise questions in relation to data minimization. Employers typically collect and process a wide range of information about employees and job applicants throughout the employment lifecycle, including recruitment documentation, performance evaluations, training records and attendance data.

In practice, minimization issues often arise during recruitment processes. Employers usually request extensive personal information from candidates at an early stage of the recruitment process, even where such information is not necessary for the initial assessment of the application.

Similar questions may arise in relation to internal employee management tools. Digital systems used for performance monitoring, time tracking or access control may generate detailed records of employee activity. Organisations should therefore assess whether the level of detail collected through such systems is proportionate to the intended purpose and whether less intrusive solutions could achieve the same objective.

To illustrate this point, organisations sometimes consider implementing biometric systems for employee identification or access control.

Biometric technologies such as fingerprint or facial recognition systems, may offer operational advantages. However, their use involves the processing of particularly sensitive personal data. From a data minimization perspective, employers should carefully assess whether such systems are strictly necessary for the intended purpose. In many situations, the same objective, such as controlling access to certain areas or recording working time, may be achieved through less intrusive measures, such as access badges or other identification mechanisms.

This illustrates how the principle of data minimization requires organisations to consider not only whether personal data is needed, but also whether the least intrusive means is being used to achieve the intended purpose.

c. Technology and IT systems

Data minimization challenges also frequently arise in the context of IT systems and digital infrastructures. Many organisations rely on technical logs and monitoring tools to ensure system security, detect incidents and maintain the proper functioning of their services.

These systems may generate large volumes of technical information, including user identifiers, IP addresses, device information or records of system activity. While such data may be necessary for security or operational purposes, organisations should assess whether the level of detail collected and the scope of logging remain proportionate to the intended purpose.

For example, some logging systems may collect detailed information about user activity by default, even where aggregated or less granular data would be sufficient to detect technical issues or security incidents. In such situations, organisations should consider whether the same objective could be achieved while processing less personal data or limiting the amount of information recorded.

d. Hospitality and tourism sector

The hospitality sector also presents specific challenges in relation to data minimization. Hotels and accommodation providers process personal data in the context of reservations, guest identification and payment processing.

Beyond these operational requirements, many hospitality businesses also collect additional information to enhance customer experience, such as guest preferences, previous stay history or special requests. While such information may support personalised services or loyalty programmes, companies should regularly assess whether all collected data remains necessary for the purposes for which it was initially obtained.

For example, guest management systems may retain detailed profiles containing historical information about previous stays, preferences or specific requests. Over time, these profiles may accumulate information that is no longer relevant to the current relationship with the guest.

From a data minimization perspective, organisations should therefore periodically review the scope of the information stored in guest profiles and ensure that only data that remains relevant for operational or customer service purposes is retained.

5. The risk of storing unnecessary data

Beyond regulatory compliance, retaining unnecessary personal data can create a range of practical risks. While retaining large datasets may appear operationally convenient, in practice it often increases both compliance exposure and organisational complexity.

One of the most immediate risks relates to information security. The more personal data an organisation collects and stores, the greater volume of information potentially affected in the event of a security incident. Data breaches frequently involve historical datasets that have been accumulated over time as a result of collecting more personal data than is strictly required. Where organisations process more personal data than required, the potential impact of a breach may increase significantly.

Processing excessive personal data can also make internal data governance more complex. Larger datasets require additional efforts to manage access rights, control data flows and ensure that personal

data is used only for the purposes originally identified. This may also complicate an organisation's ability to respond efficiently, for example to requests from individuals exercising their data protection rights.

From a regulatory perspective, collecting more personal data than necessary may also raise compliance concerns under the GDPR, particularly in light of the principles of data minimization and storage limitation. These principles require organisations to ensure that the personal data they process remains adequate, relevant and limited to what is necessary for the purposes pursued.

Finally, beyond compliance considerations, excessive data collection may also generate additional operational and financial costs. Larger datasets require more storage capacity, stronger security measures and greater governance efforts.

For these reasons, limiting the amount of personal data collected and retained should not be viewed solely as a compliance exercise, but also as an important element of effective risk management.

6. Recommendations for organisations and their DPOs/ privacy leaders

How can organisations and DPOs move from recognising data minimization risks to actively managing them in practice?

In many organisations, excessive data collection is rarely the result of a deliberate decision. More often, it is the consequence of evolving business processes, legacy systems, expanding data fields in forms, or the gradual accumulation of information across different tools and databases.

For DPOs and privacy leaders, the challenge is therefore not purely legal. It is also organisational and governance driven. Ensuring that personal data remains limited to what is necessary requires regular review of processes, systems and internal practices.

Based on our experience, the following recommendations may help organisations move from awareness to a more structured and defensible data minimization framework.

DPO checklist

1. Challenge the “collect now, assess later” mindset

Excessive data collection often stems from the assumption that additional information may be useful in the future. Organisations should ensure that each category of data is collected for a clearly defined purpose and is genuinely necessary.

2. Review data collection practices

Data minimization starts at the point of collection. Forms, onboarding processes and internal tools should be periodically reviewed to ensure that only relevant and necessary information is requested.

A simple way to support this assessment is to ask:

- Is this data strictly required for the purpose?
- Could the same objective be achieved with less or less detailed data?
- Is there a legal obligation to collect it?
- Will the data actually be used?

3. Limit access and reduce unnecessary data flows

Minimization also concerns how data is accessed and shared. Organisations should ensure that access rights and data flows are limited to what is strictly necessary for each function.

4. Integrate minimization into governance processes

Data minimization should be integrated into governance processes, including project design, internal reviews and compliance frameworks. DPOs play a key role in ensuring that this principle is applied in practice across the organisation.

5. Define and enforce retention periods

Data minimization also requires organisations to define clear retention periods and ensure that personal data is not kept longer than necessary. Retention policies should be implemented in practice, including through IT system settings and regular data cleaning exercises.

6. Raise awareness across the organisation

Effective data minimization depends on awareness across the organisation. Both IT teams and business units should understand and apply minimisation principles in their day-to-day activities, supported by regular training and awareness initiatives.

These recommendations show that data minimization is not simply a legal requirement under the GDPR, but a practical tool to reduce risk and improve data governance.

Organisations that proactively review their data practices are better positioned to reduce risks, simplify compliance efforts and strengthen their overall data governance framework.

How we can help

At Stellan Partners, our Technologies, Data & IP team supports organisations in addressing these challenges by:

- assisting DPOs and privacy teams in reviewing data processing practices,
- conducting data minimization and data governance assessments,
- reviewing internal processes, forms and systems from a data protection perspective,
- supporting organisations during CNPD inspections or regulatory reviews,
- providing tailored training on practical GDPR implementation.

If you would like to discuss how your organisation can better implement data minimization in practice, please contact a member of our Technologies, Data & IP team.



Audrey RUSTICELLI

Deputy Managing Partner

New Technologies, Data & IP

audrey.rustichelli@stellanpartners.lu

T: +352 661 463 238



Mar IBÁÑEZ ARRIBAS

Associate

New Technologies, Data & IP

mar.ibanez@stellanpartners.lu

T: +352 621 164 754

This newsletter has been prepared by Stellan Partners for general guidance only. Although the greatest care has been taken to ensure that the information contained therein are accurate on the date of publication, Stellan Partners does not accept any liability to any person for the information (or the use or reliance upon such information) which is provided in this handbook or incorporated into it by reference. On any specific matter, please contact us for appropriate advice. The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination, or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from any computer.