Data protection by design & by default: When to act and what to do

EDPB European Data Protection Board

February 2026

Data Protection by Design and by Default (DPbDD) is a cornerstone of the GDPR. It is not an option—it is a mandatory and continuous duty for **every organisation**, regardless of your organisation's size.

The goal is simple: to ensure that **privacy protection is built into your systems and processes from the very beginning** (by design) and that the default settings for any new process are the **most privacy-friendly possible** (by default).

The EDPB Guidelines on Data Protection by Design and by Default provide guidance on how to effectively implement these principles and safeguard individuals' rights throughout the lifecycle of the data processing.

Data Protection by Design

Your proactive duty. Organisations must integrate appropriate technical and organisational measures to implement all data protection principles **before** you start processing and **continuously** thereafter.

When to act	What to do
When selecting the processing method	Design security, minimisation, and consent features into all new software, hardware, and processes. **Ask yourself: Can we design this to use less data?**
During processing	Maintain, review, and update existing systems and processes to ensure they remain compliant against the latest risks and using the newest technologies. **Ask yourself: Are our current systems facing new risks?**

The four factors you must consider

When designing any system or procedure, your measures must be **effective**. To ensure this effectiveness, you must assess:

1. **Risks:** Evaluate the **likelihood and severity** of risks to individuals' fundamental rights. This risk analysis must drive your choice of safeguards.

2. **State of the art:** You should be aware of current technological progress. If a better, commercially available, and more protective technology exists, you should consider it. This applies to both **technical** measures (like encryption) and **organisational** measures (like staff training or setting up internal policies for IT governance). Controllers are encouraged to engage with their providers to be made aware of latest technological developments.

3. **Cost of implementation:** Cost is a factor, but **never an excuse** to forgo effective protection. If two measures offer equal protection, you can choose the less costly one. However, the chosen measure must always ensure compliance.

4. **Nature, scope, context, and purpose:** Tailor your data protection efforts to the specific situation. A system managing sensitive health data requires much stronger measures than one managing only public business contact information.

Data Protection by Default

Your limiting duty. By default, your systems must only process the amount of data **necessary** for each specific purpose. Users should have to **intervene** to increase the scope of data processing.

The **necessity** rule applies to four key dimensions:

Dimension	Default rule	Practical example
1. Amount of data collected	Only collect the minimum volume and level of detail required.	**Do not** make a 'Date of Birth' field mandatory on a web form if the sole purpose is to send a receipt.
2. Extent of processing	Limit the types of operations performed on the data (e.g., aggregation vs. individual profiling).	If you collect location data to show the nearest store, **do not** automatically use it for personalised advertising unless the user opts in.
3. Period of storage	Personal data must be kept for no longer than is necessary for the purpose.	Set up **automatic deletion or anonymisation** routines for data as soon as the retention period expires.
4. Accessibility	Access must be restricted to a minimal number of authorised people (**need-to-know basis**).	**Never** make data accessible to an indefinite number of people (e.g., search engines) without explicit user intervention.

Principles in practice: Key steps for business owners

The obligation to implement DPbDD requires you to operationalise all seven data protection principles: (1) lawfulness, fairness and transparency; (2) purpose limitation; (3) data minimisation; (4) accuracy; (5) storage limitation; (6) integrity and confidentiality (security); (7) accountability.

1. Data minimisation

- **Data avoidance:** Always check if you can achieve the purpose using aggregated data (statistical data combined from multiple sources where individual details are removed), anonymised data, or less granular (highly detailed or specific) data.
- **Pseudonymisation:** Pseudonymisation is the processing of personal data in such a way that the data can no longer be attributed to a specific individual without the use of additional information. Use pseudonymisation as soon as you no longer need direct identification. This significantly lowers the risks. While pseudonymisation is a valuable data minimisation technique, it should not be relied upon as a standalone solution for all scenarios.

Example

(section 3.5, page 22)

Context: A bookshop wants to boost online sales. The owner creates a mandatory-order form requiring different fields (like date of birth, phone number, and address) to be filled to complete a purchase.

What to do: Not all the info required in the form is needed for book purchases. If payment is upfront, the date of birth and phone number are not necessary unless justified. Similarly, an address is not needed for eBooks since they're downloaded digitally.

The web shop owner therefore decides to make two web forms: one for ordering books, with a field for the customer's address, and one web form for ordering eBooks without a field for the customer's address.

2. Integrity and confidentiality

This principle is about securing data against unauthorised access, loss, or damage, and it relies heavily on technical and organisational design.

- **Access segregation:** Implement a strong **Access Control Management** policy. No single person alone should have comprehensive access to all data about an individual, and no employee should have access to data they do not need to perform their duties.
- **Security by design:** Build security requirements in from the start. Use **encryption** for data storage where appropriate, and **network segmentation** for keeping sensitive data servers separate from general IT networks.
- **Incident response:** Design robust processes for detecting, containing, reporting, and learning from potential data breaches.

3. Fairness and transparency

Your relationship with the individual must be honest, neutral, and respectful.

- **Transparency by design:** Information about data processing must be **concise, intelligible, and easily accessible**. Provide information at the **relevant time** (e.g., a pop-up notice when collecting specific data).
- **Fair choices:** Do not design interfaces that confuse, deceive, or pressure users into sharing more data than they intend. For consent, the choice to **'Accept'** must be presented just as easily and visibly as the choice to **'Decline'** or **'Adjust Settings.'**

Example

(section 3.3, page 18)

Context: A streaming service offers standard and premium plans, with the premium plan including higher quality video and priority customer support.

What to do: Prioritised support for premium subscribers cannot delay or deny regular subscribers' GDPR rights (such as the right to access or erasure). While premium users may pay for faster service, the data protection-related requests of all customers must still be managed without undue delay.

The accountability checklist for small businesses

DPbDD is a key part of your **Accountability** obligation—your ability to demonstrate to regulators (and customers) that you have taken effective measures to comply. For small businesses, smart design choices are the most efficient way to meet this duty.

Your action plan for DPbDD compliance

Action point	Why it matters
1. Conduct early risk assessments	Do this before purchasing or developing any new system. It guides your design, prevents costly changes later, and demonstrates due diligence.
2. Demand guarantees from vendors	When buying software (e.g., CRM, HR, E-commerce), require the producer or processor to demonstrate how their system enables your compliance with DPbDD. This can include **certification** or adherence to relevant **Codes of Conduct**.
3. Start simple, then scale	Begin by applying the DPbDD framework to your most high-risk areas (e.g., customer financial data, employee records) and then gradually integrate the principles across your entire organisation.
4. Address legacy systems	Existing and older systems are **not exempt**. You must review them regularly. If a legacy system cannot be updated or redesigned to comply with DPbDD, it **should be promptly migrated to newer systems**.
5. Leverage expertise	If you have a Data Protection Officer, involve them actively from the design/procurement stage. Otherwise, seek advice to ensure you are meeting the 'State of the Art' requirement without overspending.

By prioritising **necessity** and ensuring that **privacy is the default** in all your operational choices, you can effectively meet your DPbDD obligations and build lasting trust with your customers.

This document provides a simplified overview of the guidelines. For more comprehensive legal explanations and examples, please consult the full guidelines.

Read the complete guidelines