

WHITE PAPER

# Navigating HIPAA

Safeguarding Health Data in the  
Data Protection Landscape



**DPO Consultancy**  
Experts in Data Privacy

AUTHORS

**Johan Martens**  
**Emine Bilsin**  
**Deniz Naz Kaya**

# Navigating HIPAA: Safeguarding Health Data in the Data Protection Landscape

## Introduction


In the pursuit of digital transformation, the United States (U.S.) Congress has undertaken efforts to enhance the efficiency of healthcare delivery. As a crucial part of this initiative, a transition from traditional paper-based to electronic reimbursements, particularly in federal healthcare payments, has been implemented. Consequently, the imperative arose to restrict the utilization of protected health information (PHI) and impose penalties on those failing to comply with confidentiality requirements.

Health Insurance Portability and Accountability Act (HIPAA) establishes limitations on the use of any data qualifying as a personal identifier by covered entities and their business associates. Covered entities encompass health plans, healthcare clearinghouses, and healthcare providers. Interestingly, the term “patients” is not explicitly included in this definition. Entities falling outside the scope of covered entities or business associates are not subject to HIPAA rules.

Covered entities are obligated to adhere to various regulatory requirements, aligning with the three primary mandates outlined by HIPAA. The first is the privacy rule, which establishes standards for the use of PHI and the right to access such information. The second is the security rule, which delineates standards for electronic transmission and storage. The third rule emphasized by HIPAA is the breach notification rule, outlining the procedures and reporting obligations that entities must follow in the event of a data breach.

## I. Background

HIPAA plays a crucial role in reshaping the health industry to align with emerging technologies and digitalization. Its inception in 1996 aimed at addressing key concerns such as reducing fraud and preventing the



abuse of healthcare providers. Although signed into law in 1996, the rules outlined by HIPAA only became effective after several years. Over the past two decades, numerous additions and amendments, including the introduction of the Privacy Rule, Security Rule, and Breach Notification Rule, have shaped its framework. Significant changes, influenced by the HITECH Act in 2013 and the Final Omnibus Rule, have further refined both privacy and security rules.

In 2011, the Office for Civil Rights (OCR) initiated a series of pilot audits to scrutinize how healthcare providers implement HIPAA Privacy and Security Rules. The audits focus on ensuring the ongoing compliance of healthcare providers with HIPAA and identifying potential shortcomings in the process.

## II. Scope and Enforcement

HIPAA Rules apply to covered entities and their business associates specifically. In other words, the regulation is not applicable for all individuals or institutions within the health sector. Moreover, the mere processing of individually identifiable health information does not automatically place an entity within the scope of these rules. HIPAA rules serve to the aim of protecting the PHI.

### Protected Health Information (PHI)<sup>1</sup>

The regulations under HIPAA are designed to ensure the adequate protection of PHI. PHI encompasses information stored in medical or designated records that can be used to identify an individual. It is present in various forms, including computer files, paper records, insurance records, provider information, and legal office records.

---

<sup>1</sup> Unlike the “personal data” in GDPR which refers to any information relating to an identified or identifiable natural person (GDPR Article 4(1)).

### Covered Entity

HIPAA rules apply to covered entities, which can be classified under three categories. The first one is a health plan which refers to an individual or group plan that provides or pays the cost of medical care. They include health insurance companies, health maintenance organizations, government programs that pay for healthcare, and military and veterans' health programs.

The second one is a health care clearinghouse and it refers to a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks. In addition to this definition, to be considered a health care clearing house, it should either be processing or facilitating the process of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction or receiving a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

The last covered entity under HIPAA rules is the health care provider. This is a provider of services and any other person or organization who furnishes, bills or is paid for health care in the normal course of business. Healthcare providers include hospitals, clinics, doctors, psychologists, dentists, chiropractors, nursing homes, pharmacies, home health agencies, and other providers of healthcare that transmit health information electronically.

### Business Associate<sup>2</sup>

Given the complexity of healthcare activities, covered entities may require business services. HIPAA also encompasses these services, safeguarding health data privacy. For such services to qualify as a business associate, the information must only be used to supplement the covered entity, not for independent purposes. This leads to the introduction of a new term, namely a business associate.

A person or entity who, on behalf of a covered entity, performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information is called a business associate. Business associates are also persons or entities performing legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity where performing those services involves the disclosure of individually identifiable health information by the covered entity or another business associate of the covered entity to that person or entity. A member of a covered entity's workforce is not one of its business associates. A covered entity may be a business associate of another covered entity.

---

<sup>2</sup> A similar term in the GDPR is the processor, which means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

### Business Associate Agreement

The covered entity and the business associate are required to sign a contract named business associate agreement (BAA). The elements that should be included in the agreement between a business associate and a covered entity are established in 45 CFR 164.504(e).

The Business Associate Agreement must describe the permitted and required PHI uses by the Business Associate. In addition to this, it should provide that the Business Associate will not use or further disclose PHI other than as permitted or required by the contract or as required by law and also require the Business Associate to use appropriate safeguards to prevent inappropriate PHI use or disclosure. There are some exemptions established in HIPAA concerning the business associate agreement requirement.

### Enforcement Authority

HIPAA operates at the federal level, enforced by the Office for Civil Rights (OCR) within the Department of Health and Human Services (HHS). OCR holds the authority to penalize non-compliant covered entities with fines of up to \$50,000 per violation. Criminal aspects of violations fall under the purview of the Department of Justice. OCR oversees compliance reviews and primarily addresses complaints. Upon receiving a complaint, OCR initiates an investigation, involving both the complainant and the implicated covered entity. If the complaint involves criminal activity, OCR forwards it to the Department of Justice; otherwise, OCR proceeds with the investigation. In case of a violation, civil money penalties are imposed, and the covered entity may request a hearing to contest the sanction.





### III. Extraterritorial Application of HIPAA<sup>3</sup>

The purpose of HIPAA is not to have an extraterritorial reach. In other words, HIPAA is not aimed to be applied beyond the U.S. borders, meaning its main object is to protect PHI of U.S. citizens regardless of their geographical position. HIPAA is de facto applicable outside the U.S. Briefly, if a company engages with the PHI of even a single U.S. citizen, HIPAA comes into effect, regardless of the company's location.

### IV. Protection of Protected Health Information (PHI) under HIPAA

Eighteen identifiers are designated as PHI. However, these identifiers alone are not considered as PHI. To be considered as one, they should be paired with health information as well. The identifiers in question are:

1. Names
2. Date of births (excluding the year)
3. Telephone numbers
4. Geographic data
5. FAX numbers
6. Social Security numbers
7. Email addresses
8. Medical record numbers
9. Account numbers
10. Health plan beneficiary numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plates
13. Web URLs
14. Device identifiers and serial numbers
15. Internet protocol addresses
16. Full-face photos and comparable images
17. Biometric identifiers (e.g., retinal scan, fingerprints)
18. Any unique identifying number or code

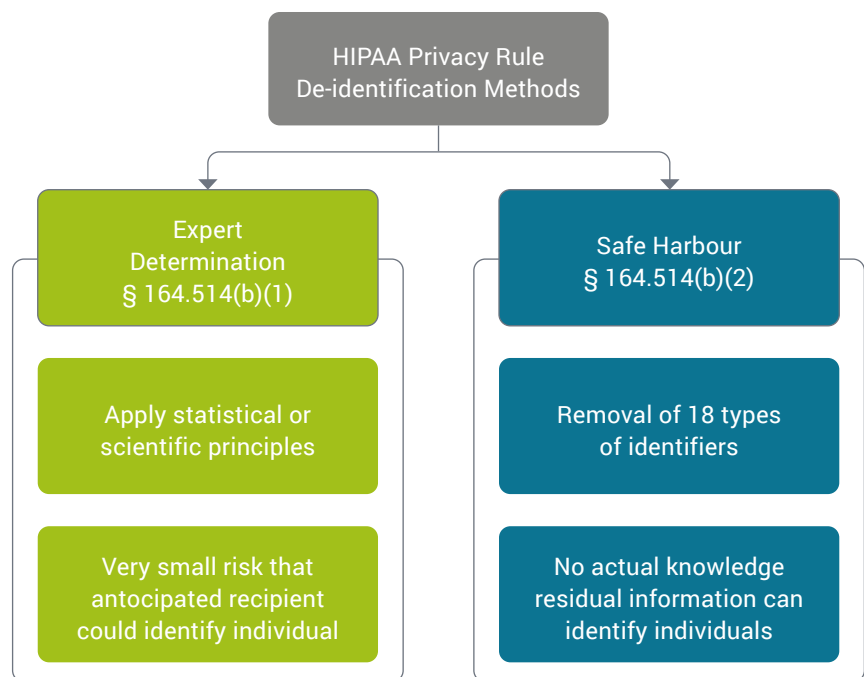
<sup>3</sup> There is a different scenario for GDPR. Any organization that processes personal data within the European Union will fall under the scope of the GDPR. In addition to this, a non-EU organization can fall in the scope of the GDPR when offering goods or services to individuals in the EU (GDPR, Article 3).

<sup>4</sup> On the other hand, GDPR introduces anonymization, defined as the process of rendering personal data anonymous to the extent that the data subject is no longer identifiable. When personal data is properly anonymized, it ceases to be considered personal data under the GDPR (Recital 26 of the GDPR). True anonymization is a high bar to meet as it must not be possible to identify the data subject for data to be properly anonymized. However, the GDPR does not provide express instructions for how to anonymize personal data.

Individually identifiable information, by itself, is not PHI. To constitute PHI, and thereby be subject to regulation by HIPAA, PII must relate to health status. It must be created, collected, transmitted, or maintained by a covered entity concerning the provision of healthcare, payment of healthcare, or use in healthcare operations activities.

#### De-Identification Methods under HIPAA Privacy Rule<sup>4</sup>

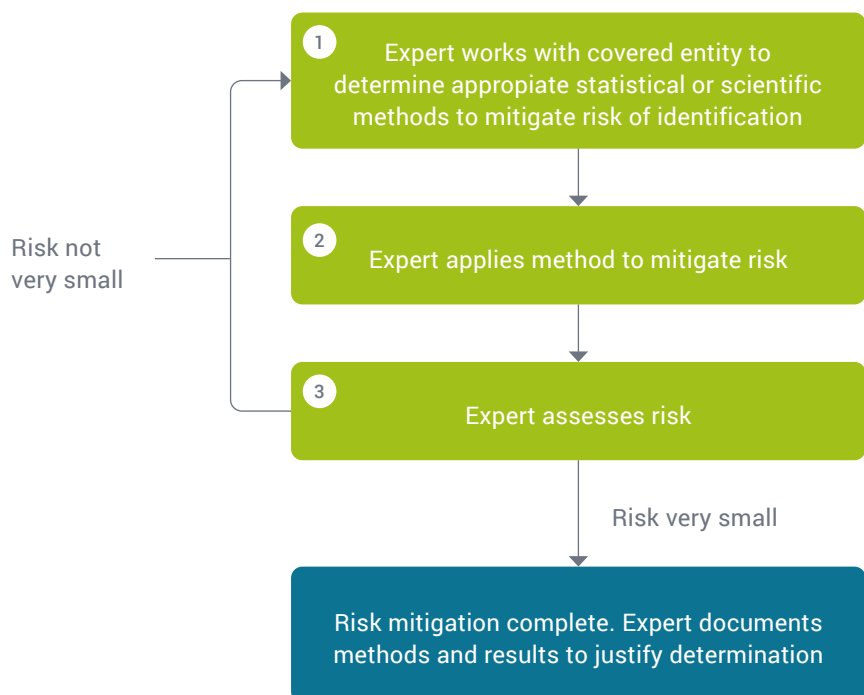
HIPAA's Privacy Rule includes two methods for de-identifying health information, allowing it to be exempt from the Privacy Rule's protections.



#### Expert Determination Method:

To be an expert, no specific degree or certification is mandated.

Experts assess the risk of data being “linked” to a source revealing individual identities. Conditions for linkage include data uniqueness, a naming data source, and a relational mechanism between de-identified and identified data.





### Safe Harbor Method:

Identifiers are completely removed in accordance with this method.

The important aspect of this method is to remove all the identifiers; not parts of them.

By satisfying either method, a covered entity demonstrates compliance with the HIPAA Privacy Rule's de-identification standard, ensuring that the information is exempt from the Privacy Rule's protections. De-identified health information, following either method, is no longer protected by the Privacy Rule as it falls outside the definition of PHI.

## V. Rules

### HIPAA Privacy Rule: Safeguarding Confidential Health Information

This rule assures individuals that their PHI will not be disclosed without their explicit consent. The HIPAA Privacy Rule specifically shields "individually identifiable health information," often referred to interchangeably as PHI. According to the guidelines set by the HHS, this encompasses information related to an individual's past, present, or future physical or mental health or condition. Additionally, it extends its protection to information about the provision of healthcare to the individual and the past, present, or future payment for healthcare provision to the individual. The rule explicitly excludes de-identified health information from its purview.

### Limitations and Authorizations

A primary objective of the Privacy Rule under HIPAA is to clearly define and restrict the circumstances under which an individual's PHI may be utilized or disclosed by covered entities.

Covered entities are prohibited from using or disclosing PHI, except under two conditions: (1) as explicitly permitted or mandated by the Privacy Rule, or (2) with the written authorization of the individual who is the subject of the information or the individual's representative.



*Required Disclosures:*

A covered entity is compelled to disclose PHI in only two scenarios. (1) to individuals or their representatives, particularly when they request access to their PHI or seek an accounting of disclosures, and (2) to the HHS during a compliance investigation, review, or enforcement action.

*Permitted Uses and Disclosures:*

A covered entity is granted permission, though not obligated, to use and disclose PHI without the need for individual authorization in several situations: (1) To the Individual (2) for Treatment, Payment, and Health Care Operations (3) Providing individuals with the chance to consent or object (4) Incidental disclosures within permissible actions (5) Instances where disclosure serves public interests (6) For research, public health, or healthcare operations. Covered entities can exercise professional ethics and judgment in determining which permissive uses and disclosures are appropriate.

*HIPAA Authorization: Ensuring Consent and Privacy*<sup>5</sup>

A HIPAA authorization is the explicit consent granted by an individual, allowing a covered entity or business associate to use or disclose the individual's PHI to a third party for a purpose that would otherwise be restricted by the HIPAA Privacy Rule. For the authorization to be valid, it must be in writing, presented in clear language, and must encompass specific elements and statements.

The elements that must be a part of the authorization should primarily include the description of PHI which will provide the outlining of PHI involved. The name of the Authorizing Person as well as the name of the Authorized Person or Organization must be specified. In addition to this, the purpose of use or disclosure should be described. Establishing a date after which the authorization is no longer valid is crucial as well. Lastly, the signature of the Authorized Person is needed for a valid authorization.

In addition to the elements, some statements have to take place as well. The first one is the right to revoke. Acknowledging the individual's right to revoke the authorization in writing at any time and providing details on the revocation process is an important part. Another statement is Non-Conditionality. This statement refers to the clarification that the individual's treatment, payment, enrollment, or eligibility for benefits is not contingent upon signing the authorization. Lastly, the re-disclosure notice statement provides the information that any data disclosed as per the authorization may be re-disclosed by the recipient and loses protection under federal or state health privacy laws.

---

<sup>5</sup> Different from the consent in GDPR, which is mandatory for the processing of personal health data (which falls under sensitive data). However, the data may be processed without consent if it meets one of the conditions of processing in Article 9 of the GDPR and a legal basis applies.

If any of the specified elements or statements are absent, the authorization is deemed invalid and should be returned to the individual for correction. This stringent framework ensures that individuals provide informed and comprehensive consent, safeguarding their privacy while allowing for necessary disclosures under HIPAA regulations.

### **HIPAA Privacy Notice: Ensuring Transparency and Compliance**

The HIPAA Privacy Rule mandates health plans and covered health-care providers to develop and disseminate a notice that offers a clear, user-friendly explanation of individuals' rights concerning their personal health information and the privacy practices of health plans and health-care providers.

The Privacy Notice must be written in plain language and cover essential aspects, including:

- How the Privacy Rule permits providers to use and disclose PHI, emphasizing the necessity of authorization for other purposes.
- The organization must safeguard health information privacy.
- Individual privacy rights, including the right to complain to the HHS and the organization for privacy violations.
- Contact information for further inquiries and complaints.

Health plans must provide the Privacy Notice to new enrollees at the time of enrollment. Furthermore, at least once every three years, plans must either redistribute the Privacy Notice or notify participants of its availability with instructions on obtaining a copy. Self-insured health plans must create and provide their Privacy Notices, while fully insured plans have special rules where the health insurance issuer takes primary responsibility. The Privacy Notice must be provided within 60 days of a material change or upon a participant's request. If a revised notice is sent, the three-year notice requirement resets.

Moreover, the Privacy Notice must be delivered directly to individuals covered by the plan. Electronic delivery is permissible with participant consent, but a failed electronic delivery requires a paper copy to be provided. If the plan maintains a website, the Privacy Notice must be posted and electronically accessible through the site.

### **Minimum Necessary Principle<sup>6</sup>**

Covered entities must make reasonable efforts to employ, disclose, or request only the minimum amount of PHI necessary to achieve the intended purpose. Covered entities must implement policies and procedures to reasonably restrict uses and disclosures to the minimum necessary. The minimum necessary standard applies to any use, disclosure, or request for PHI. Covered entities cannot use, disclose, or request an entire medical record unless it is specifically justified as reasonably needed for the intended purpose.

<sup>6</sup> There is similar principle in the GDPR, namely data minimization principle. It means that a data controller should limit the collection of personal information. It is slightly different from HIPAA given that minimum necessary principle mainly restricts the uses and disclosures, instead of the collection of the data. There are also different principles in GDPR such as the right to be forgotten, ensuring the individuals' right to have their data deleted upon request.

### **HIPAA Security Rule: Safeguarding e-PHI**

The Security Rule sets national standards to protect specific health information. Unlike the Privacy Rule, which focuses on individuals' rights to access and control their PHI, the Security Rule is concerned with safeguarding electronic protected health information (e-PHI) created by covered entities and business associates. Covered entities must ensure confidentiality, integrity, and availability of e-PHI.

When adopting the safeguards under the security rule, the covered entities must pay attention to some specific concepts such as size, complexity, and capabilities; technical, hardware, and software infrastructure; costs of security measures; likelihood and possible impact of potential risks to e-PHI.

The Security Rule outlines three categories of safeguards; administrative, physical, and technical. In addition to these safeguards, a covered entity must maintain, for six years, written security policies and procedures, as well as written records of required actions, activities, or assessments, extending from the creation or last effective date.

Administrative Safeguards in the HIPAA Security Rule include but are not limited to the Security Management Process, which leads covered entities to identify and analyze potential risks to e-PHI. Another safeguard under the same category is designating a security official responsible for developing and implementing security policies and procedures. Information Access Management is also important for implementing policies and procedures for authorizing access to e-PHI based on the user's role (role-based access). Workforce training and management is another beneficial safeguard that supports the supervision of workforce members handling e-PHI.

Physical safeguards in HIPAA security rules include facility access and control, which means limiting physical access to facilities in which only personnel are authorized.

Workstation and device security are another physical safeguard, engaging in the development of policies and procedures for the proper use and access to workstations and electronic media.

Establish guidelines for the transfer, removal, disposal, and re-use of electronic media to ensure the protection of e-PHI may be provided as examples.

Technical Safeguards in the HIPAA Security Rule include but are not limited to access control which refers to implementing technical policies and procedures to ensure that only authorized individuals have access to e-PHI. Audit controls are for utilizing hardware, software, and procedural mechanisms to record and examine access and other activities within information systems containing or using e-PHI. On the other hand, integrity controls implement policies and procedures to prevent unauthorized alteration or destruction of e-PHI.

### **Breach Notification Rule in HIPAA: Key Points<sup>7</sup>**

A breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI. HIPAA covered entities and their business associates must provide notification following a breach of unsecured PHI.

Any disclosure of health information is considered a breach unless the covered entity or business associate demonstrates a low probability of compromise through a risk assessment. Therefore, conducting a risk assessment is almost always important to determine the steps to be taken. The factors considered in a risk assessment include the nature and extent of the involved PHI, including identifiers and the likelihood of re-identification; identification of the unauthorized person or recipient of the disclosure; whether the PHI was acquired or viewed; extent to which the risk to PHI has been mitigated.

The Breach Notification Rule emphasizes the importance of promptly notifying affected individuals and relevant authorities when a breach of unsecured PHI occurs. The risk assessment helps determine the likelihood of compromise, guiding the appropriate response and mitigation efforts.

Following a breach of unsecured PHI, covered entities and business associates have specific notification obligations to several organizations and people, namely, to the individual, to the Secretary, and the media under certain circumstances.

Covered entities must notify affected individuals promptly, within 60 days of discovering the breach. Notification can be in written form through mail or email, depending on the preferences agreed upon with the individuals. If contact information is insufficient for 10 or more

<sup>7</sup> GDPR requires that breaches other than the ones which are unlikely to result in a risk to the right and freedoms of natural persons must be reported to a designated GDPR regulator within 72 hours. In HIPAA the duration is 60 days, which is far longer.

individuals, substitute notice methods are required, such as posting on the entity's website or in major media. The notice should include details about the breach, types of information involved, steps for individuals to protect themselves, and actions taken by the entity to investigate and prevent future breaches.

Covered entities must report breaches to the Secretary of the HHS by electronically submitting a breach report form. If the breach affects 500 or more individuals, the covered entity must notify the Secretary without undue delay and within 60 days of discovering the breach. For breaches affecting fewer than 500 individuals, covered entities can report these breaches to the Secretary annually, with reports due no later than 60 days after the end of the calendar year in which the breaches were discovered.

Covered entities experiencing a breach affecting more than 500 residents of a specific state or jurisdiction must provide notice to prominent media outlets serving that area. Media notification, often in the form of a press release, must be delivered promptly within 60 days of discovering the breach. The media notice should include the same information as the individual notice, describing the breach, types of information involved, steps for affected individuals to protect themselves, and actions taken by the entity to address the breach.





## Conclusion

In conclusion, the U.S. Congress' commitment to digital transformation within the realm of healthcare has manifested through a strategic shift from traditional paper-based processes to electronic reimbursements, particularly in federal healthcare payments. The significance of this transition is underscored by the imperative to safeguard PHI, leading to the enforcement of stringent measures against non-compliance with confidentiality requirements.

At the core of this regulatory landscape is the HIPAA, which plays a pivotal role in delineating the responsibilities and limitations of covered entities and their business associates. Noteworthy is the explicit focus on data privacy, electronic security, and breach notification procedures, encapsulated in the three primary mandates of the HIPAA framework.

As the healthcare industry navigates the complexities of digital transformation, the continued adherence to HIPAA regulations becomes paramount. The emphasis on protecting patient information, coupled with the electronic evolution of reimbursement processes, reflects a concerted effort to enhance both the efficiency and security of healthcare delivery. In this dynamic landscape, the evolving role of HIPAA stands as a critical pillar, guiding the trajectory of healthcare digitization in the United States.

## Bibliography

- Centers for Disease Control and Prevention (CDC). (2022). Health Insurance Portability and Accountability Act (HIPAA). Retrieved from <https://www.cdc.gov/phlp/publications/topic/hipaa.html>.
- Centers for Medicare & Medicaid Services (CMS). (2023). Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security: HIPAA Basics for Providers: Privacy, Security, & Breach Notification Rules. Retrieved from <https://www.cms.gov/outreach-and-education/medicare-learning-network-mln/mlnproducts/downloads/hipaaprivacyandsecurity.pdf>
- U.S. Department of Health & Human Services. (1996). Health Insurance Portability and Accountability Act (HIPAA). Retrieved from <https://www.hhs.gov/hipaa/index.html>.
- U.S. Department of Health & Human Services. (2022). Laws & Regulations: Health Insurance Portability and Accountability Act (HIPAA). Retrieved from <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html>.
- IAPP, 'GDPR Vendor Management: We've Seen This Movie Before' <https://iapp.org/news/a/gdpr-vendor-management-weve-seen-this-movie-before/>
- EDPS (European Data Protection Supervisor), 'Data Minimisation' [https://www.edps.europa.eu/data-protection/data-protection/glossary/d\\_en#:~:text=The%20principle%20of%20%E2%80%9Cdata%20minimisation,necessary%20to%20fulfil%20that%20purpose](https://www.edps.europa.eu/data-protection/data-protection/glossary/d_en#:~:text=The%20principle%20of%20%E2%80%9Cdata%20minimisation,necessary%20to%20fulfil%20that%20purpose)



Europalaan 28b  
5232 BC 's-Hertogenbosch  
The Netherlands

Congresstraat 35  
1000 Brussels  
Belgium

1 Lyric Square London  
W6 0NB  
England

+31 850 711 080  
info@dpoconsultancy.nl  
[www.dpoconsultancy.com](http://www.dpoconsultancy.com)



**DPO Consultancy**  
Experts in Data Privacy