WHITE PAPER

Applying Privacy by Design in practice: a starter's guide

JUNE 2022

Dounia Skalli

Introduction

"If you do Privacy By Design, you will gain a competitive advantage."

Dr. Ann Cavoukian, (former Information and Privacy Commissioner of Ontario, Canada).[1]

Privacy by Design (hereinafter: PbD) originated in the early 1990s and is an engineering and strategic management approach that allows you to selectively and sustainably minimize information system's privacy risks through technical and organizational controls. Since the introduction of the GDPR, the philosophy of PbD is also reflected in article 25, requiring organizations as data controllers to implement data protection by design and by default.

The origin of Privacy by Design

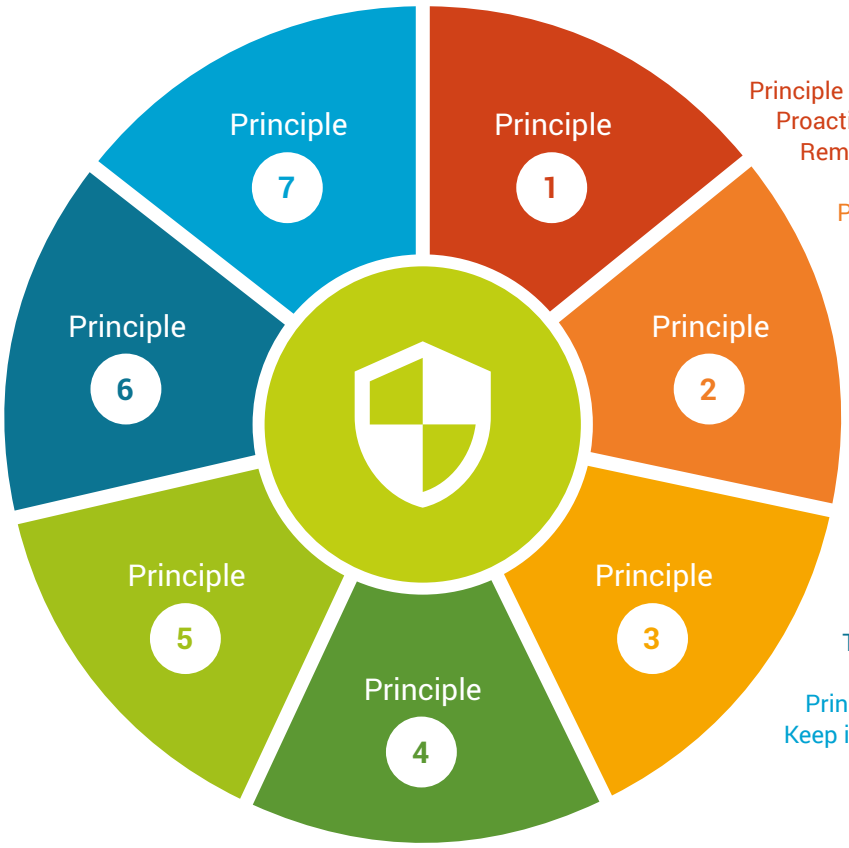
Dr. Ann Cavoukian developed the modern conceptualization of Privacy by Design because she believes privacy should be embedded into information technologies (IT), business practices, and networked infrastructures, as a core functionality. This leads to two major advantages:

- Competitive advantage: Organizations that tell their customers the lengths that you are going to protect and respect their privacy will breed loyalty and consequently attracts new opportunities, for example by attracting new customers, which ultimately leads to competitive advantage.
- Cost-efficiency: When applying Privacy by Design, it also allows you to work in a cost-efficient manner. Since you include technical and organization controls to mitigate privacy risks in an early design stage, which prevents that you have to make expensive adjustments later on while developing for example a product or service.

The total of 7 Foundational Principles form the embodiment of the PbD Principle. PbD should be interpreted as an information system design philosophy on how to improve the user-friendliness of IT systems and technologies. Therefore, the practical outcome of implementing the PbD principles within each organization may differ vastly and it depends greatly on the particular circumstances involved.

1 https://www.nonconformistinnovation.com/ann-cavoukian/, April 7, 2019.

The aim of this guidance is to provide an explanation, tips, and examples on how to practically implement PbD within your organization, by *defining* each principle, *what* accompanied actions belong to each principle, and *how* the actions can be achieved.[2]



Principle 1:
Proactive not Reactive; Preventative not Remedial

Principle 2:
Privacy as the Default Setting

Principle 3:
Privacy Embedded into Design

Principle 4:
Full Functionality – Positive-Sum, not Zero-Sum

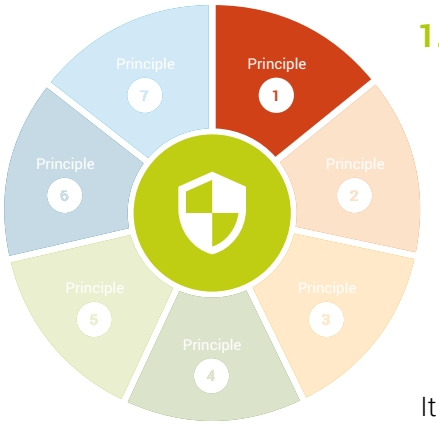
Principle 5: End-to-End Security – Full Lifecycle Protection

Principle 6: Visibility and Transparency – Keep it Open

Principle 7: Respect for User Privacy – Keep it User-Centric

2 *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices*, Ann Cavoukian, Ph.D., December 2012, p. 7-11.

1. Principle 1: Proactive not Reactive; Preventative not Remedial



1.1 Principle 1: Definition

The first principle of PbD includes the importance of having a proactive and not a reactive approach in any product, service, system or process. The aim should be to prevent that privacy risks will materialize. PbD expects you to anticipate and implement proactive measures to prevent privacy invasive events from occurring, instead of offering remedies for solving such events.

It is essential that organizations start with an executive-led approach that explicitly recognizes the values and benefits of proactively adopting strong privacy practices, early on in the process and in a consistent manner. Clear commitments and resources allocated to back them up, are necessary to develop a culture of privacy across the entire organization. At all levels, privacy should be incorporated into the daily operations of an organization.

To achieve this culture, there should be clearly identified business owners accountable who take on lead responsibility. The business owner may be involved in different roles, such as privacy leaders, business process owners, project leaders, or executives.

1.2 Principle 1: What actions can you take?

Under this PbD Principle, there are 4 actions that you can take to implement a proactive approach in into your product, service, system or process:

1. Affirm senior leadership commitment to a strong, proactive privacy program.
2. Ensure that concrete actions, not just policies, reflect a commitment to privacy. Monitor through a system of regularly reviewed metrics.
3. Develop systematic methods to assess privacy & security risks and to correct any negative impacts, well before they occur.
4. Encourage privacy practices demonstrably shared by diverse user communities and stakeholders, in a culture of continuous improvement.

Ideally, leadership or senior management are responsible for conducting these actions as they should carry responsibility.[3]

1.3 Principle 1: How can you achieve the actions?

With this Principle it is important to commit to a privacy-friendly processing of personal data, and to enforce it. This can be done by implementing the following proactive measures per action:

Action 1

- Set up privacy governance within the organization by aligning with senior leadership and the installment of a privacy team to assure that the relevant departments are involved in the privacy management activities.
- Ensure that directors receive appropriate privacy training and that there are board members with privacy expertise. Education is key. Otherwise, they would not be able to ask the right questions about privacy practices.
- At least one senior manager must be designated to be accountable for the organization's privacy compliance.

Action 2

- Choose a privacy framework that suits your organization, such as the Nymity Privacy Framework or the NOREA Privacy Control Framework. The privacy framework will allow you to track progress of privacy management activities and to report in a well-structured way frequently on the needed privacy management activities.
- Set up a privacy policy/statement and make resources available to implement the policy.
- Implement a privacy policy that reflects the privacy needs and risks.
- Link each privacy policy component to a concrete action item that should be executed.
- Demonstrate how each practice item will be implemented.

3 Idem, p. 13-14.

- Leadership should ask senior management to undertake periodic privacy self-assessments and privacy audits and to frequently report to the board on these activities.
- Designate a 'go-to' person for privacy-related queries within the organization.

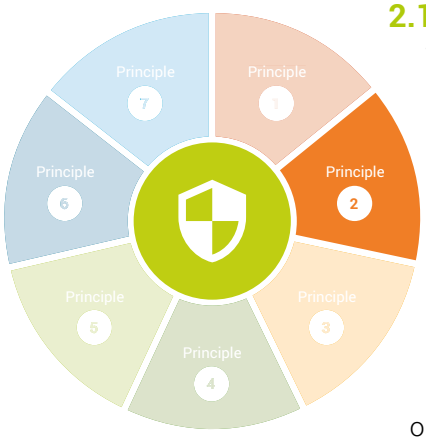
Action 3

- Implement systematic methods to perform privacy risk assessments and data protection impact assessments and perform them to assess risks.
- When reviewing or updating software (new versions) you need to make sure that privacy is taken into consideration when adding or improving functionality. When new technologies are used, privacy has to be addressed because the privacy implications of new technologies are often not known early on.

Action 4

- Set up an education program in which you work on awareness and training throughout the organization while considering different levels of training based on different roles within the organization.
- Privacy has to become a part of the development process. For example, when developing products for customers, every developer has to include privacy when discussing new products with our clients.

2. Principle 2: Privacy as the Default Setting



2.1 Principle 2: Definition

The second principle is about setting privacy as the default setting. Users need to be able to trust one thing – the default settings. As a starting point, organizations can provide maximum privacy assurance to personal data in any of their IT systems or business process without any further action that is needed on the side of the individual whose data is being processed. When the need for or use of personal information is not clear, there is a presumption of privacy and the precautionary principle applies: the default settings are the most privacy-protective. If your organization builds privacy into the system and process, the data is automatically protected by default.

An essential element when designing privacy-enhancing systems and processes, is to always respect the data purpose limitation principle under the GDPR. Meaning, that you should only process personal data if you have a specific purpose for which you need to process that data. This purpose should be narrow, clear, limited, relevant, and specific enough.

Another essential element is to include the data minimization principle under the GDPR as well. You should only process the personal data you actually need to achieve the specific purpose you set for processing personal data. This is important because this way you prevent processing an excessive amount of data, which results in less privacy risks therefore less harm.

2.2 Principle 2: What actions can you take?

This principle includes 4 actions that you should complete to implement this principle in your organization's systems and processes:

1. Adopt purposes that are as narrow and specific for processing personal data as possible.
2. Minimize the processing of personal data to a data set that is necessary to achieve the set purpose.
3. Limit the use of personal data to the specific purpose for which it was collected originally.
4. Create policy, technological and procedural barriers to prevent that data can be linked to personal information.

3 Idem, p. 21-22.

Regarding responsibility, ideally software engineers and developers would be concerned to adopt purposes (action 1), since the individuals fulfilling these roles are able to decide the specific purposes in an early stage of a project.

Furthermore, application and program owners are able to focus on data minimization (action 2) and use limitation (action 3), since they are more knowledgeable on the actual system or application and therefore know how to implement these two actions.

Lastly, since the line of business and process owners have the best overview on the process, they can create barriers to prevent linkage of data.[4]

2.3 Principle 2: How can you achieve the actions?

To achieve the actions above, you can think of the following measures per action:

Action 1

- Create and implement a process in which privacy expertise is always involved when it comes to the adoption and assessment of narrow and specific purposes. Specified purposes should be clear, limited and relevant to the circumstances.
- A record of processing activities is highly recommended and for some mandatory because it creates insight into all the different specific purposes per processing activity. Besides, involving privacy expertise allows you to keep the record of processing up to date when it comes to your organization's processing activities.

4 Idem, p. 21-22.

Action 2

- Always ask yourself if you can reasonably achieve the same purpose with less data. If the answer is yes, the data is 'nice to have' and not 'necessary' to achieve the set purpose. The collection of personally identifiable information should be kept to a strict minimum.
- A great way to assess this is to include a section for personal data elements in your privacy risk assessment, data protection impact assessment or legitimate interest assessment and to describe per data element what the necessity exactly is.

Action 3

- It is recommended that you create an overview of the different data elements and document the specific purpose for which the data was originally collected. This allows you to assess whether a purpose is compatible with the original purpose to begin with.

Action 4

- You can process or collect personal data in different separated databases or systems.
- You can distribute the processing of data across different physical locations.
- To delete (partial) personal data that is no longer needed.
- To create and implement an authorization process.

3. Principle 3: Privacy Embedded into Design

3.1 Principle 3: Definition

The basis of the principle is that privacy should be included as an essential component in the design and architecture of IT systems and business operations. This means that privacy should be included from the very beginning in which core functionality is delivered, and not something you include as an 'add-on' in a later stage of the design process.

To be able to implement this principle, you can think of clearly documenting all the interests and objectives, including privacy, to articulate desired functions, the agreed upon and applied metrics, and trade-offs that are rejected as being unnecessary. This all should be in favor of finding a solution that enables multi-functionality (see principle 4: Full Functionality – Positive Sum, not Zero-Sum).

Also important, is to realize that PbD cannot be viewed exclusively as an 'IT project', but privacy expertise should be available and engaged throughout all phases to combine a multi-faceted understanding of privacy issues and requirements with the appreciation of consumer/client expectations. Besides, it might be the case that complex situations demand the need for competencies of functional experts, risk managers, or other specialists.

3.2 Principle 3: What actions can you take?

The accompanied 4 actions aim to embed privacy requirements in the architecture and design of IT systems and business operations:

1. Perform a privacy risk assessment in the design stage of any initiative within the organization.
2. Base identity metasystems on the "Laws of Identity", intended to codify a set of fundamental principles that universally adopted and sustainable identity architecture must adhere to.
3. Consider privacy in organizational engineering processes and system development lifecycles.
4. Embed privacy into regulatory approaches that are guided by flexibility, common sense and pragmatism, in the form of self-regulation, omnibus privacy legislation, sectoral privacy laws and more general legal frameworks.

When it comes to responsibility, application and program owners are well-suited to perform a privacy risk assessment, and therefore to assess for example what unintended uses of personal information might come into play when designing the technical architecture of a system (action 1).

The line of business and process owners are able to base identity metasystems on the "Laws of Identity" because of their knowledge and overview of the particular process (action 2).

Software engineers and developers are perfectly able to make sure that privacy is considered in the engineering processes and system development lifecycles because they own this process for a major part (action 3). This does not mean that privacy is a barrier to any innovation, system designers should be encouraged to practice responsible innovation in the field of advanced analytics.

Lastly, regulators have the responsibility and possibility to embed privacy into regulatory approaches that are guided by flexibility, common sense and pragmatism (action 4).[5]

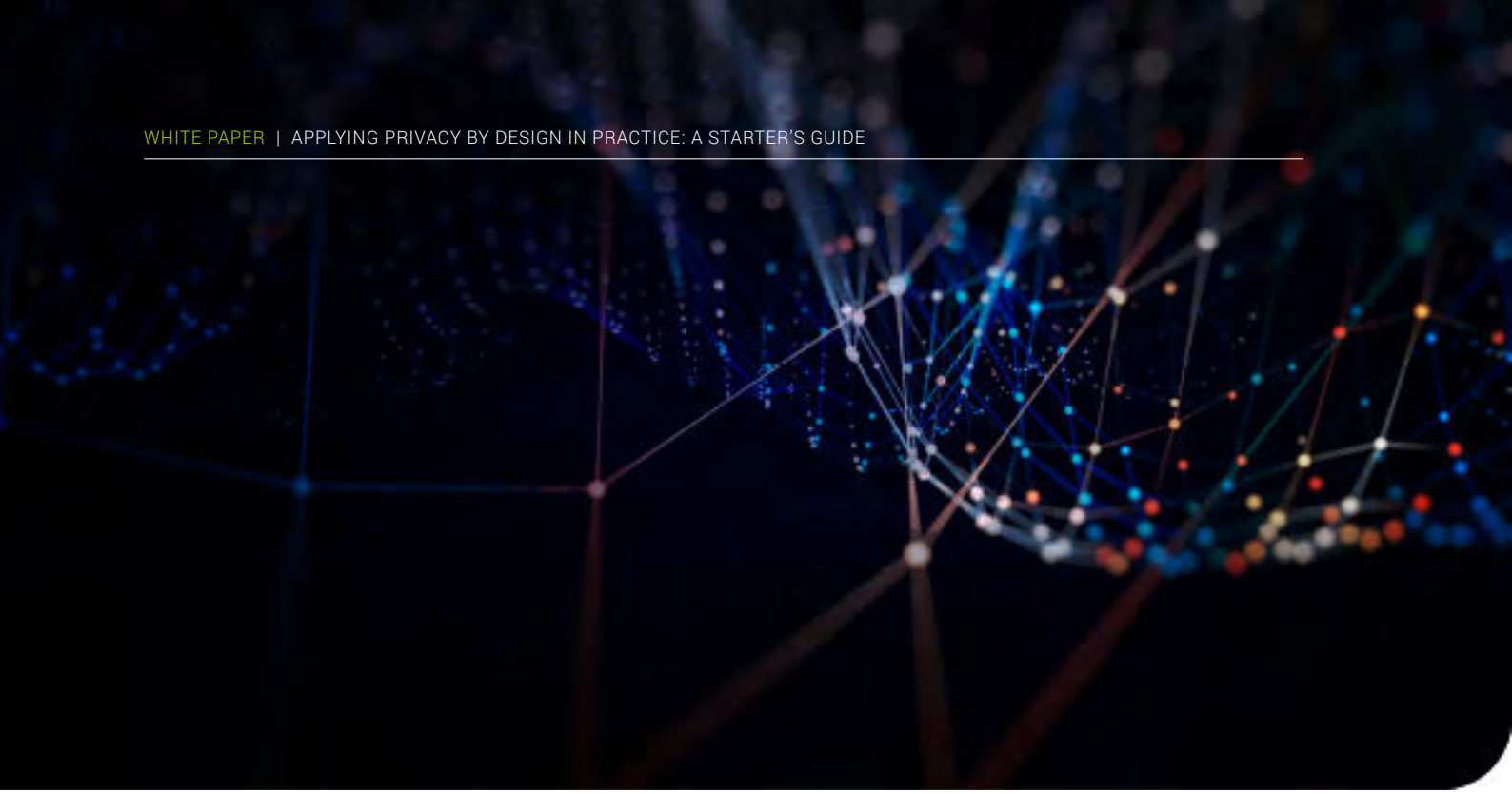
3.3 Principle 3: How can you achieve the actions?

Except for the 4th action described above, your organization is able to take further action when it comes to action 1-3:

Action 1

- Involve privacy expertise to make sure a privacy risk assessment is adequately conducted. Discuss the privacy of your products or tools with your peers. When questions are raised do not brush them aside with "It will be fine" or "It really is not that bad".
- Create and implement a privacy risk assessment standard to adequately assess privacy risks in a consistent and decent manner.

5 Idem, p. 26-27.



Including considerations of alternatives and the selection of different or less metrics.
- Create and implement a policy and procedure in which privacy expertise is included in the design stages of new initiatives within the organization.

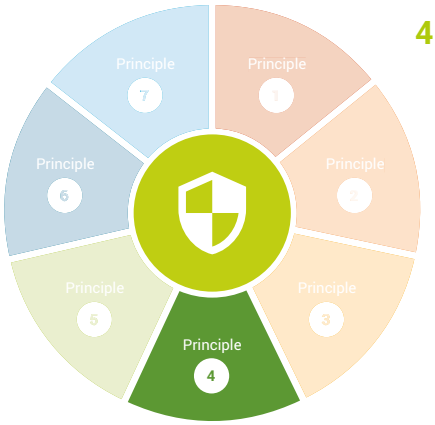
Action 2

- Set and implement the fundamental principles to which universally adopted and sustainable identity architecture must conform. The role of identity metasystems is to provide a reliable way to establish who is connecting with what system. A unifying identity metasystem is of great value because it can protect applications from the internal complexities of specific implementations and allows fundamental principles to be conformed.

Action 3

- Create a policy and procedure in which privacy expertise should be included in the new development or evaluation of engineering processes or system development.
- When engineering processes or system development, consider important privacy elements, such as the purpose of processing data, the retention term, what data is required, the security measures and use limitation of the data.

4. Principle 4: Full Functionality – Positive-Sum, not Zero-Sum



4.1 Principle 4: Definition

This principle aims to accommodate legitimate interests and objectives in a 'win-win' manner, rather than an approach that makes unnecessary compromises with privacy. It rejects the zero-sum view that privacy should be sacrificed if you are aiming for other design objectives, legitimate interests, and/or technical capabilities. It stimulates a positive-sum approach in which you will have a doubly-enabling outcome with privacy in mind.

This principle suits especially in cases where there are conflicting needs within the organization. For example, if you are developing a digital marketplace, you want customers to be able to easily buy and check-out products with minimal effort. But you also want to respect the data minimization principle by only processing the data you necessarily need to finalize the sale of your product, meaning with the least possible amount of data. Instead of asking for the customer's financial data to finalize the sale, the organization could also secure the payments via a third-party vendor. This way, the commerce team would still allow a smoothened buying process, while the organization does not collect any financial customer data, and therefore respects data minimization under the GDPR.

4.2 Principle 4: What actions can you take?

The following 3 actions will stimulate a positive-sum approach:

1. Acknowledge that there are multiple, legitimate business interest that should coexist.
2. Practice the 3 C's, communication, consultation and collaboration, to better understand multiple, and sometimes divergent interests.
3. Achieve multiple functionalities by pursuing innovative options and solutions.

The responsibility with acknowledging coexistence of multiple, legitimate business interests, lies with the leaders or senior management of the organization. It is most important to have leaders that understand, support and send an unmistakable signal to the organization that you do

not have to choose between privacy and other legitimate interests. This is crucial if you want to generate support throughout the organization for a positive-sum approach (action 1).

The responsibility for action 2 lies with the application & program owners, but also with the line of business and process owners. By practicing the 3 C's and working closely together they are able to achieve a positive-sum result together, because these are the roles that are most knowledgeable on the different interests involved.

Furthermore, action 3's responsibility lies with the software engineers and developers. These are the individuals that know about all the different innovative options and solutions, and combine and balance them with the different legitimate interests involved.[6]

4.3 Principle 4: How can you achieve the actions?

Practical measures that can be taken to implement the actions described above are:

Action 1

- Leaders and/or senior management should create a statement that translates the message that privacy and other legitimate interest can coexist in their privacy strategy documentation.
- They should also carry out this message in other suitable situations, such as presentations, meetings and conversations within the organization.
- Give successful examples of how this has been managed before to make it more practical for the organization.

6 Idem, p. 33-34.

- When you create a product or service, do not state that privacy is not possible because the technical capabilities of the product do not allow for certain privacy enhancing technologies. You have to ensure that the product is capable of protecting the privacy of your end users.

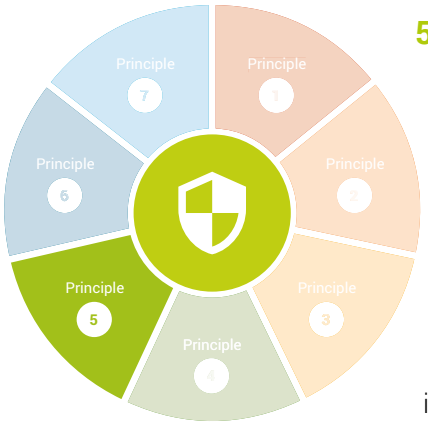
Action 2:

- Especially for application and program owners & business and process owners, it is important to create a process that starts with creating an overview of the legitimate interests/stakes and stakeholders involved.
- By having an overview of the legitimate interests/stakes and stakeholders involved, you can work on clear communication lines, and to consult and collaborate with the necessary stakeholders.
- You can then determine what may be divergent interests and work closely together in a balanced collaboration to create a positive-sum environment, in which you can compensate but in which you always strive for a 'win-win'-result.
- What can help achieve this result is to organize multiple meetings throughout the process, including all the stakeholders, and to document the outcomes clearly.

Action 3:

- It is important to be aware of and list the functionalities that have the highest priority.
- The people most knowledgeable about these functionalities and the technology behind them are best suited to find innovative options and solutions to look for alternatives, and should work closely together if you come across any barrier regarding privacy vs. functionality.
- You have to aim for solutions that have multi-functionality, driving sales while also making sure privacy is at the heart of what you do.

5. Principle 5: End-to-End Security – Full Lifecycle Protection



5.1 Principle 5: Definition

The goal of the fifth principle is to ensure that data is secured and destroyed in a timely manner throughout the entire lifecycle management. Throughout its entire lifecycle data should be secured from end-to-end, at rest, in transit, and while in use. Furthermore, this should be consistent with international standards that have been developed and recognized.

It is important to comprehend that data security is essential to information privacy, but it does not equal privacy because data security is about how the data is protected. It may be compared with a chain because it is only as strong as its weakest link.

5.2 Principle 5: What actions can you take?

The following 3 actions can be taken to implement this principle:

1. Aim to make the state of data if breached 'unreadable' by default, meaning encrypted.
2. Deploy encryption carefully and correctly to integrate it into your devices and workflows as smoothly as possible.
3. Ensure that personal data is destructed and disposed of at the end of its lifecycle.

The responsibility of action 1 lies with software engineers and developers, since the individuals in these roles are most knowledgeable on how to make sure that data is encrypted during the complete lifecycle of data.

Application and program owners are most-suited when it comes to deploying encryption correctly and carefully into the devices and workflows, since they are aware on how to integrate the encryption with the well-known applications and workflows.

Lastly, the line of business and process owners, are mostly aware of the complete process and lifecycle of the data. They know exactly what moment during the process the data should be destructed and disposed of.[7]

7 Idem, p. 38-39.

5.3 Principle 5: How can you achieve the actions?

The practical measures that can be taken include the following:

Action 1:

- When designing a process or device that collects, stores and or processes personal data you ensure that personal information is securely processed and transmitted.
- Employ encryption by default to mitigate security risks throughout the lifecycle and ensure the data is unreadable in case there is loss, theft or disposal of data, for example when a laptop is stolen, or a smartphone is lost.
- Use a trustworthy encryption system with a minimum standard for the protection of data and that uses keys that are very large numbers. The most common symmetric algorithm in use today, AES, is typically used with keys that are 256 bits in size.
- You transmit data using secure https connections employing the highest TLS version possible.

Action 2:

- Use encryption keys that are of a sufficient length in order to resist attempts to break the encryption.
- Encryption keys must be protected to prevent them from being stolen or disclosed to unauthorized individuals.
- Secure the authentication of users to ensure that only authorized individuals can decrypt and access the data.
- Ensure that no copy of the decrypted data exists unless an authorized user intentionally created one.
- Authorized users should be provided with adequate training in how they can access and protect the encrypted data.
- Encrypted data should remain available by a centralized management of passwords and other authentication tokens, but also by backing up the encrypted data.

- Performing risk assessments on IT infrastructures that use security technologies, such as encryption, allow you to ensure that it works as expected before it is going live.

Action 3:

- Create a destruction of data policy that outlines in advance what records should be destroyed, by whom, and when.
- Include in the destruction policy details regarding the methods of in-house or outsourced destruction activities, and contingency planning.
- Segregate records that should be destroyed, and securely store them throughout the process, before and after destruction.
- When deciding on the method of destruction, you should consider:
  - The medium in which the record is stored;
  - Whether the data requires a stronger method of destruction based on the sensitivity of the data; and
  - What will happen with the media afterwards: being reused internally or moved out of the organization.
- Recycling records and simply placing them in the trash bin are non-acceptable methods of destruction, avoid both.
- When employing a service provider that will securely destroy the data, it is important to have the required elements in place, such as performing a due diligence on this provider and to have the needed formal agreements in place.
- It is recommended to perform an audit on the secure destruction programs to ensure compliance.

6. Principle 6: Visibility and Transparency – Keep it Open

6.1 Principle 6: Definition

It is very important that the technology or business practice involved is transparent to the user, that it is aligned with the objectives that are stated and shared with individuals, and that it is subjected to independent verification.

Both visibility and transparency are essential when it comes to establishing accountability and trust for all stakeholders involved. It is important to have trust but there should also be verification.

6.2 Principle 6: What actions can you take?

There are 6 actions that can be taken to implement this principle:

1. Make sure that the identity and contact information of the responsible persons for privacy and security is available to the public and that it is well-known within the organization.
2. Use 'plain language' in public-facing policies and procedures that is easily understood by the individuals whose information is the subject of these documents.
3. Provide readily available information regarding policies, procedures, and controls relating to the management of personal data to all individuals.
4. Consider publishing summaries of risk assessments and independent third-party audit results.
5. Create a list that contains the personal data that is held by the organization.
6. Create audit tools to ensure that users can easily determine how their data is used, protected, and stored. But also to determine whether the policies are properly enforced.

The responsibility for actions 1 and 2 lies with the leaders/senior management of the organization. They are in the position to include the necessary identity and contact information in the required documentation and to also make this well-known within the entire organization. Furthermore, with the help of software engineers they can easily set a 'plain language' standard for public-facing policies and procedures.

For actions 3 and 4 the application developers can play a big part when it comes to making the policies, procedures and controls available. But also with the publication of summaries of risk assessment and third party audit results. Systems architects could furthermore help to establish the summaries risk assessments in which they are involved.

Lastly the system architect is also responsible for actions 5 and 6, since they have the knowledge on what personal data is maintained in the IT infrastructure of the organization. But they also can make audit tools to provide users with a tool that makes the data handling part more transparent.[8]

6.3 Principle 6: How can you achieve the actions?

There are several measures that you can implement to make sure that the above-mentioned actions are taken:

Action 1:

- The contact information of responsible persons for privacy and security can be included in the accompanied policies internally, such as in the internal privacy policy document, the information security document, and a data breach policy.
- Think of including the contact information in a privacy statement for external publication.
- Besides policies, this contact information is also efficient to include in training and awareness internally to make sure that the information is well-known within the organization.

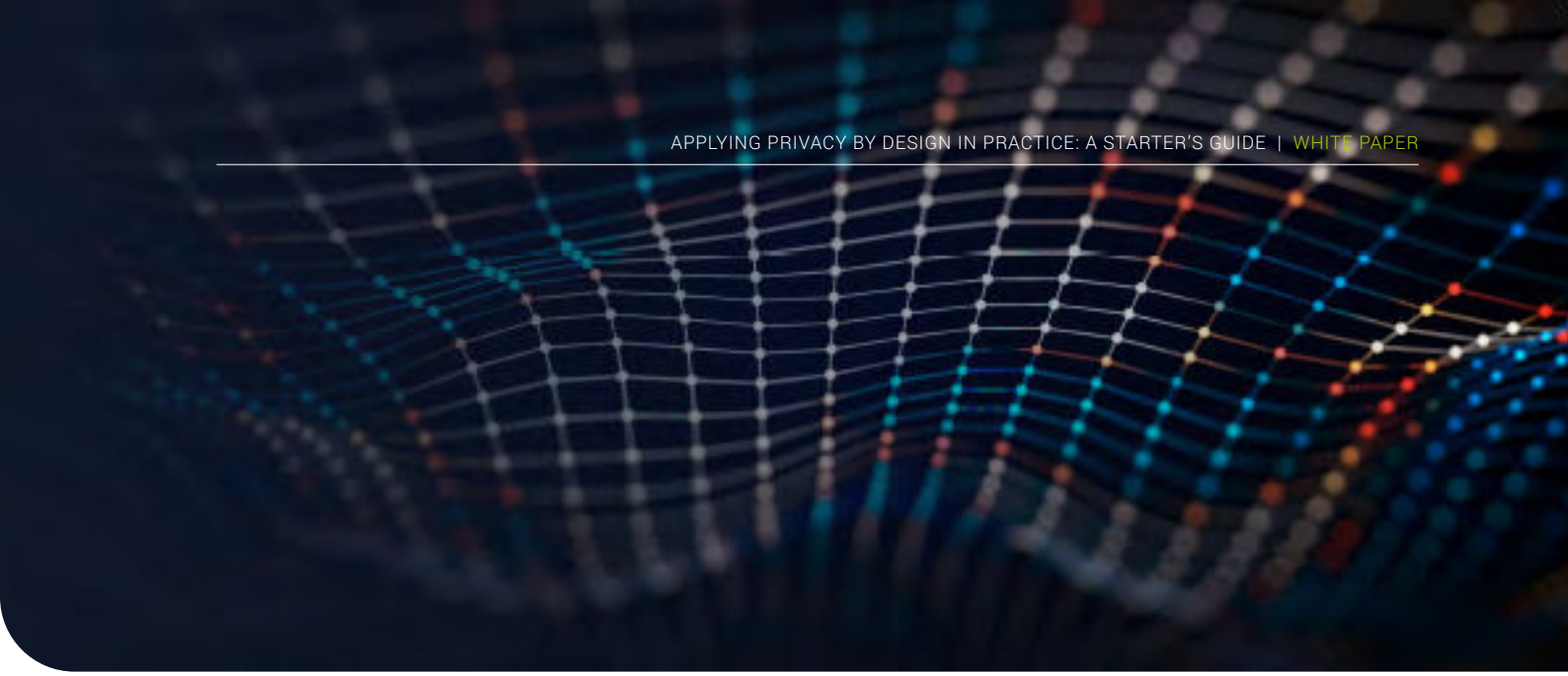
Action 2:

- Openness and transparency are key to accountability. Make information about the policies and practices relating to the management of personal information readily available to individuals.
- Introduce a policy that describes the 'plain language' standard that is used by the organization.
- Depending to which audience the documentation is aimed, you can set different standards to make it an easily readable and understandable piece.

Action 3:

- Create an environment in which internal users can easily retrieve information regarding policies, procedures, and controls relating to the management of their data, such as a shared drive or intranet.
- For external users, it can also be made available easily available by categorizing certain topics or making them easy to find, for example by providing the privacy policy on every web page on your organization's website. It can also be an FAQ categorized by topic.

8 Idem, p. 44-46.



Action 4:

- Being Accountable. The collection of personal information entails a duty of care for its protection. Responsibility for all privacy-related policies and procedures shall be documented and communicated as appropriate and assigned to a specified individual. Publishing summaries of assessments done within the organization, such as privacy impact assessments or data protection impact assessments, provides transparency and visibility for individuals to see the outcome of the data handling practices by the organization.
- Publication of a summary regarding a third-party audit report is a great way to provide independent insight into the business practices involved.

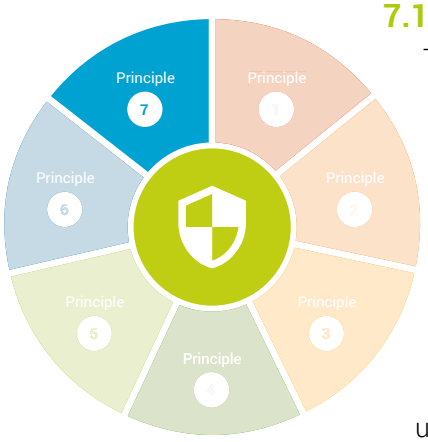
Action 5:

- Creating a list of data that is retained by your organization helps individuals to understand the processing activities involved.
- It is recommended to include this list both in an internal privacy policy and external privacy statement accompanied with explanatory descriptions on different elements of the processing activities involved, such as the purposes for which it is processed, how long it is retained, and with which parties it is shared.

Action 6:

- The audit tool provides the individual with the possibility to verify the usage, protection, and storage of the data. This tool can have many formats, it could be an informative document showing the data processing activities, but it could also be an application in which the information is displayed.

7. Principle 7: Respect for User Privacy – Keep it User-Centric



7.1 Principle 7: Definition

This principle focuses on measures in an information system that are strong privacy defaults, appropriate notice and empowering user-friendly options to keep it user-centric. This means that a system should be designed for the user, anticipating on his or her privacy perceptions, needs, requirements, and default settings.

Respecting a user means that when an information system is designed or deployed, the individual's privacy and user interests are accommodated, right from the outset. It should be possible for users to gain insight into the business operations and functioning of any system or technology that they are interacting with in real time.

The best Privacy by Design results are usually those that are consciously designed around the interests and needs of individual users, who have the greatest vested interest in the management of their own personal data.

Empowering data subjects to play an active role in the management of their own data may be the single most effective check against abuses and misuses of privacy and personal data.

7.2 Principle 7: What actions can you take?

Actions that can be taken are:

1. Offer strong privacy defaults.
2. Provide an appropriate notice to the individual.
3. Consider user-friendly options:
   a. To provide users with access to data concerning them;
   b. To make user preferences persistent and effective; and
   c. To provide access to the information management practices of the organization.

The responsibility of actions 1 and 2 lies with the leadership/senior management, since they are in the position to make decisions on what privacy defaults should be used throughout the organization. Furthermore, appropriate notice is also their responsibility, since they are accountable to properly inform the individuals involved regarding the processing activities.

For the user-friendly options different individuals are responsible. Providing users with access to the data concerning them can be arranged by application and program owners, since they are fully aware on the application's functionalities. The software engineers and developers are well-equipped to create user preferences that are persistent and effective in information systems. Lastly, the line of business and process owners are aware and can provide access to the data lifecycle and the accompanying data handling practices.[9]

7.3 Principle 7: How can you achieve the actions?

The following measure can be taken per action:

Action 1:

- Implement measures to assure transparency of the data handling practices, such as real time access to a system that the user is interacting with.
- A good example on how to offer strong privacy defaults is to create a user-centric identity management metasystem to stimulate a unified user experience that spans over different devices that are used (from desktop to mobile phones), and which allows the user to quickly determine for example what information will be revealed to which parties and for what purposes. It provides a great tool to set minimal disclosure by default for a defined purpose, and any secondary use of the information should be optional.

Action 2:

- Make sure that you inform the end user or data subject about his or her privacy rights under the GDPR.
- Provide an appropriate notice to sufficiently inform the individual on all the required data processing components provided under article 13 of the GPDR with a clear and easily understandable description in the privacy statement.
- The notice can also be shared with the individual in another way, for example by email, as long as it is provided before the start of the data processing.

Action 3:

- An example of user-friendly options is to provide making effective redress mechanisms available to individuals, such as providing an online form to easily make use of your right to access, deletion or correction of data. Redress mechanisms should not be cumbersome for individuals. Therefore, it is important that the form should not be to excessive in the number of required fields for example.

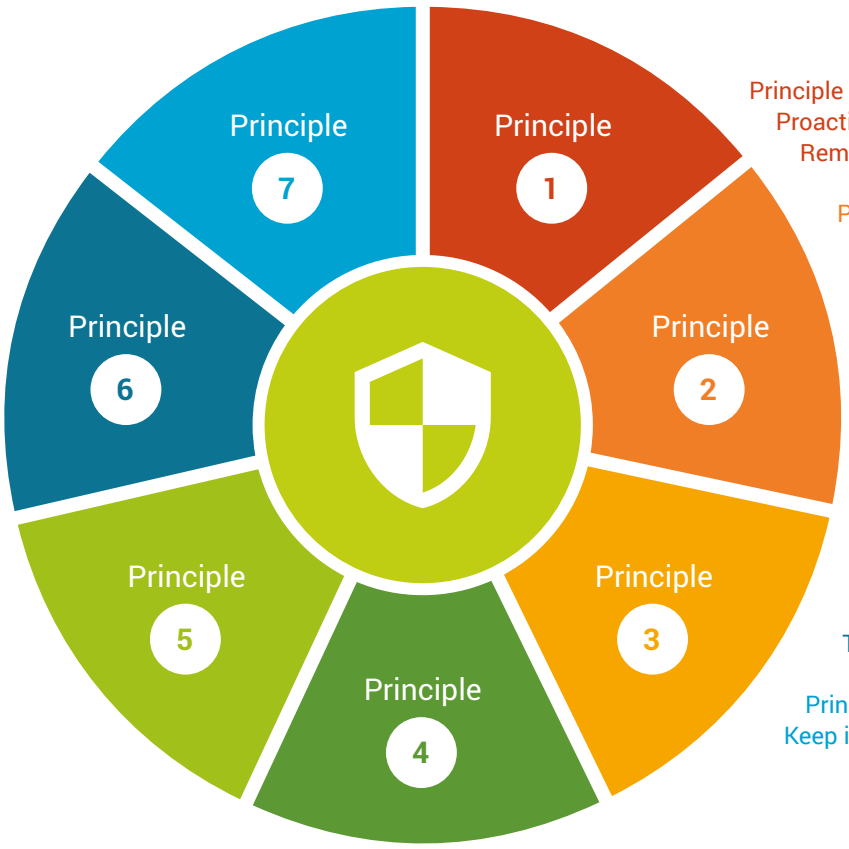
9 Idem, p. 49-51.

Start with understanding and above all doing

Privacy by Design is still quite a challenge for many organizations because it often remains too abstract and theoretical. The fact is that data privacy and data protection will only become more important in the coming years. The amount of data inside and outside your organization is growing exponentially. As a result, it is becoming increasingly complex to keep control over which personal data you process and to identify and prevent challenges in an early stage, instead of repairing them afterwards.

Privacy by Design is therefore not a 'nice to have', but a 'need to have'. It is important to proactively implement this principle when processing personal data. More and more organizations have taken the step towards Privacy by Design and are now reaping the benefits. These organizations have kept their privacy risks to a minimum, while performing business operations in a privacy-friendly and cost-efficient manner. Besides, they are aware of the latest developments in the state-of-the-art technology. As a result, the GDPR no longer feels mandatory, but it actually provides them with benefits. They build trust with customers and suppliers and breed loyalty, resulting in new opportunities to expand the customer database. And last but not least, they incur lower costs, without sacrificing the reliability and quality of their privacy management.

What these successful companies have in common is that they have immersed themselves in the theory of Privacy by Design, but also have not waited too long to act. Step by step they have applied Privacy by Design in their organization. We hope that this white paper has provided you with sufficient tools to take the first step with your organization to put Privacy by Design into practice.



Principle 1:
Proactive not Reactive; Preventative not Remedial

Principle 2:
Privacy as the Default Setting

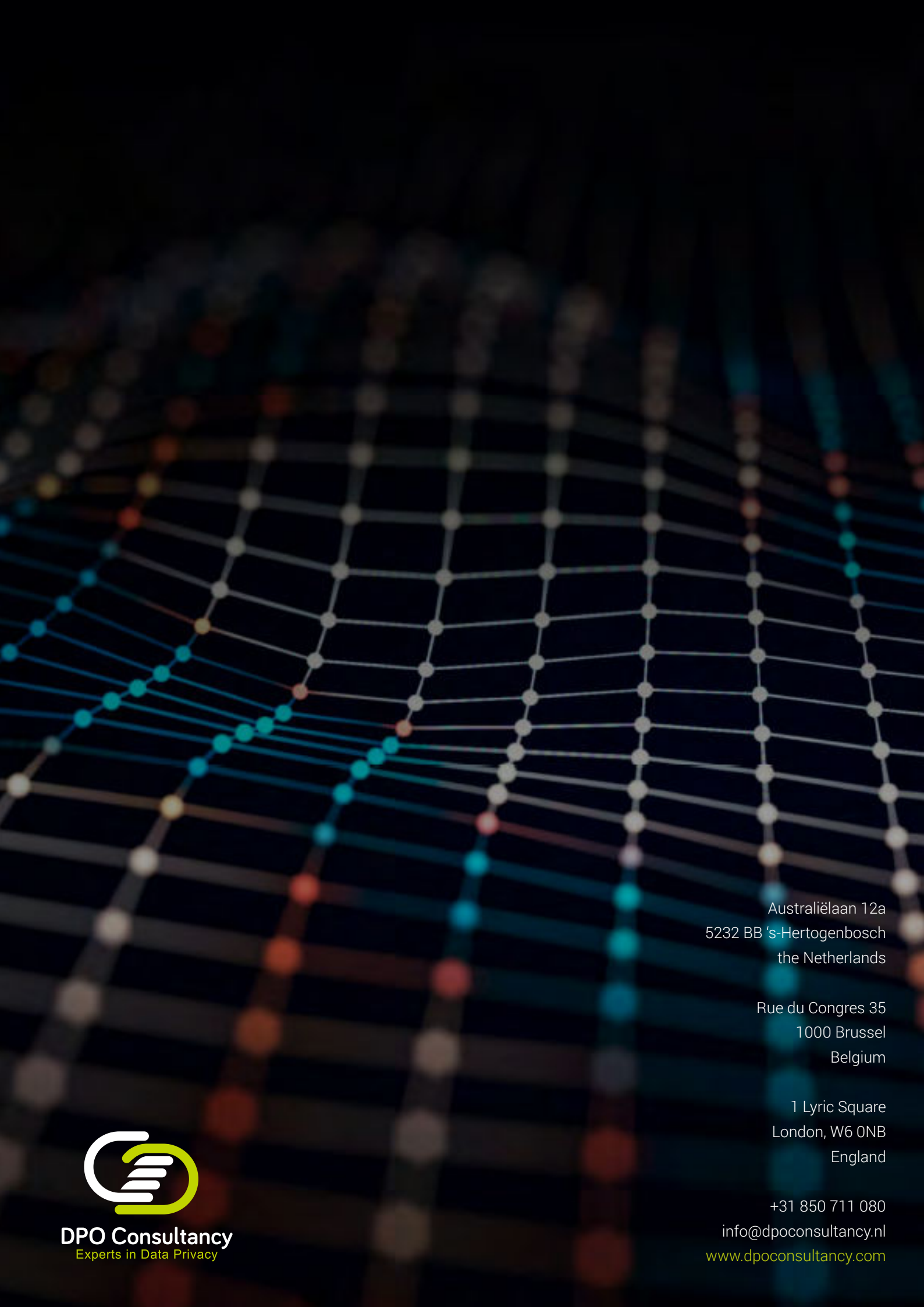
Principle 3:
Privacy Embedded into Design

Principle 4:
Full Functionality – Positive-Sum, not Zero-Sum

Principle 5: End-to-End Security – Full Lifecycle Protection

Principle 6: Visibility and Transparency – Keep it Open

Principle 7: Respect for User Privacy – Keep it User-Centric



DPO Consultancy
Experts in Data Privacy

Australiëlaan 12a
5232 BB 's-Hertogenbosch
the Netherlands

Rue du Congres 35
1000 Brussel
Belgium

1 Lyric Square
London, W6 0NB
England

+31 850 711 080
info@dpoconsultancy.nl
www.dpoconsultancy.com