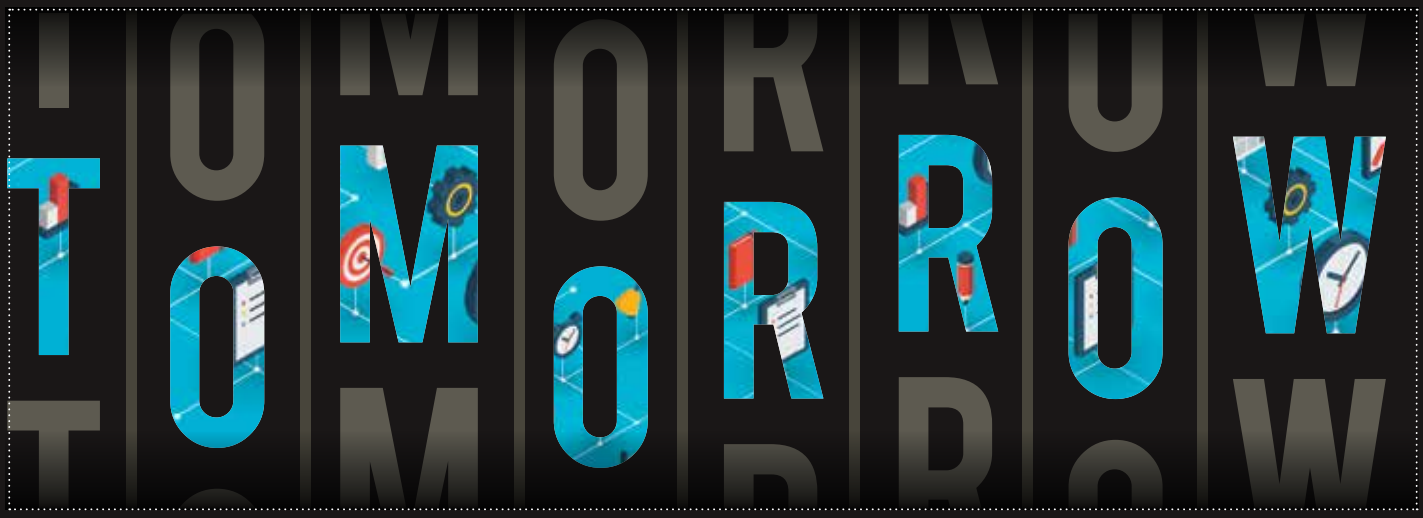
PERSPECTIVES FOR



HOW NEW TECHNOLOGIES ARE TRANSFORMING PRIVACY BY DESIGN AND BY DEFAULT

By Allison Mulford, Joseph Srouji, and Thibault Mechler

It's an understatement to say companies still have trouble effectively implementing privacy by design. Either businesses do not acknowledge, or just fail to understand, the requirements under the accountability regime of the EU General Data Protection Regulation (GDPR). It is not yet a reality to designate a data protection officer (DPO) who can operate seamlessly across the organization with independence and credibility to drive the privacy program; neither is creating awareness and partnership with information technology (IT) specialists to drive privacy initiatives in the face of challenging development goals.

But it is possible to transform an otherwise mediocre privacy program into one that is best-in-class. Given the interconnectivity between privacy and rapidly changing technology — especially IT security standards — it is no surprise that Privacy Enhancing Technologies (PET) are rising in popularity. PETs allow organizations of all sizes and resources to respond to basic GDPR accountability requirements by permitting them to imbed privacy considerations into product design and marketing strategies from the outset.

This article begins with a refresher of the legal framework of privacy by design and by default with special attention to the sanctioning regime applied to organizations that have misunderstood or otherwise ignored privacy considerations during development efforts. It then explains how PETs fit into privacy by design and by default and presents tools that allow organizations to account for requirements like data subject consent, personal data tracking (for data subjects) and control (for data controllers), data minimization, and anonymity. The article concludes with an accountability reminder that PETs are only as good as the organizational measures in place to support them.

CHEAT SHEET

- *PETs.* Privacy Enhancing Technologies (PETs) allow organizations to imbed privacy considerations into product design and market strategies, responding to EU General Data Protection Regulation (GDPR) requirements.
- *By design and default.* Privacy by design requires privacy to be incorporated into the design of IT systems and business practices without diminishing functionality. Privacy by default requires the protection of personal data to be integrated into systems, like a default setting.
- *Fines.* If data controllers do not comply with GDPR, then the EU Supervisory Authorities may impose significant fines.
- *Right choice.* Organizations need to first understand their data flows, risk profile, and relationship with third parties before determining which PETs will be most helpful.

Privacy by design and by default

Article 25 (1) of GDPR provides that data controllers "shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures … **designed** to implement data protection principles … and **to integrate the necessary safeguards** into the processing …"[1]

This provision illustrates one of the fundamental goals of GDPR: to ensure that data controllers fully integrate privacy considerations into technology developments and strategic plans. The notion of "privacy by design" is therefore met when organizations factor in privacy at each stage of data processing, from conception to use.

GDPR does not stop with privacy *by design*. Article 25 (2) also creates an obligation of privacy *by default*. Controllers shall process "only personal data [that] are necessary for each specific purpose of processing." Thus, the data, which needs to be processed for a specific purpose, should be identified before the processing starts.

In its December 2018 recommendations, the European Union Agency for Cybersecurity (ENISA) highlights the fact that privacy by design and by default "fall within the overall notion of privacy engineering" and "are closely interlinked with security of processing" of Article 32 of the GDPR. Since GDPR came into force on May 25, 2018, and in contrast to the previous legal framework under Directive 95/46/EC, privacy by design and by default are now an enforceable legal obligation.[2]

The regulatory perspective

The information and privacy commissioner of Ontario, Canada, Ann Cavoukian, is given credit for having coined the term "privacy by design" when she outlined seven foundational principles of privacy. She explained that privacy requirements should be "embedded into the design and architecture of IT systems and business practices … without diminishing functionality."[3] The second of the foundational principles of privacy, privacy as a default setting, emphasizes that ensuring protection of personal data must be integrated into systems by rule, thus building privacy into the default settings for all systems and business practices.[4]

For the UK regulator, Information Commissioner's Office (ICO), and most EU Supervisory Authorities, these are indeed the underlying concepts of privacy by design and by default. But while the notions of privacy by design and by default are now explicit obligations under GDPR, they existed well before it. The Data Protection Directive 95/46/EC, which was replaced by GDPR in 2018, contained elements of privacy by design in Recital 46, which highlighted how the technical and organizational measures should be applied "both at the time of the design of the processing system and at the time of the processing itself."[5] The ICO noted, "Privacy by design was good practice under the Data Protection Act 1998, data protection by design and by default are legal requirements under the GDPR."[6]

The risks of getting it wrong: Sanctions

If data controllers do not comply with GDPR then significant administrative fines may be imposed by EU Supervisory Authorities. Article 58 of GDPR provides the corrective powers available to supervisory authorities, including fines. Worst case administrative fines for noncompliance with GDPR can be up to €20 million or four percent of global turnover.[7]

EU Member State Supervisory Authorities have the discretion to sanction organizations but have been fairly restrained (with a few exceptions). The 2018 Annual Report of the French *Commission nationale de l'informatique et des libertés* (CNIL) illustrates the growing trend among Supervisory Authorities, namely increases in enforcement actions and fines."[8]

The new frontier of PETs

PETs are intrinsically linked with privacy by design and by default. But what are PETs, and what do they signify? A passing trend or something with much more potential? PETs can essentially be summarized as "quality basic building blocks"[14] for engineering privacy, in particular for online users who are afforded greater control over how their personal data are used online. They "embody fundamental data protection principles."[15]

Allison Mulford is vice president of legal affairs for Prometric, a US-based company in the test administration industry. *allison.mulford@prometric.com*

Joseph Srouji is *avocat à la cour* and data protection officer based in Paris, France. *joseph.srouji@sroujiavocats.com*

Thibault Mechler is a graduate law student at Université Paris II – Panthéon Assas. *mechler.thibault@gmail.com*

So PETs can be thought of as something that "reduces or eliminates the risk of contravening privacy principles within the context of ever-changing technology."[16]

PETs can have various natures and take different forms. ENISA identified four categories: secure messaging, virtual private networks, anonymizing networks, and anti-tracking tools for online browsing.[17]

PETs can serve as technology levers to increase a data subject's control over their personal data and how they can reinforce the principle of data minimization as well as privacy protection (through anonymization). The analysis is grouped into two blocks: control over personal data and protecting privacy.

Control over personal data

Data subject consent and control over one's personal data

The question of consent is closely linked to the lawfulness of the processing principle.[18] ENISA notes that, "to enable lawful data processing of individuals' personal identifiable information, individuals need to give specific, informed and explicit indication of their intentions."[19] By developing a new product that collects and processes personal data, controllers and processors need to adopt tools or technologies allowing data subjects to manage their consent. Data controllers are currently far from this ideal of allowing data subjects to effectively manage their consent; the more common approach is one of "take it or leave it" apps or contracts. PETs fill this gap, providing much-needed transparency that allows data subjects to manage their consent, which is exactly what GDPR intended.

The current best practice is allowing data subjects to provide consent for the collection and processing of certain categories of personal data and not for other categories. In practice, this can be nearly impossible to manage but with PETs it is now feasible (even if not always desired from a data controller perspective). Personal Data Stores (PDS), for example, allow data subjects to decide what information to share or not. PDS are basically "consumer-facing apps and services which can be supported by different kinds of PETs" and "enable a distributed system, where the data is stored and processed at the "edge" of the system rather than centralised."[20] This distributed approach essentially facilitates a data subject's ability to access, modify, and delete their data while offering greater protection from hackers who often target core systems. The distributed approach is a sort of safe locker for personal data maintained separately from the main IT system.

But a data subject is only able to effectively provide consent if provided with full transparency on what personal data are collected and how they will be used, hence transparency is of utmost importance. This is where some large technology companies have come under fire from EU regulators — most notably Google and Facebook — for how they use personal data for commercial purposes not necessarily disclosed in a clear way to data subjects. Here again, PETs have a role to play. In its 2014 report, ENISA highlighted different types of PET tools or functionalities that are essentially transparency-enhancing techniques (TETs). These technologies "place users in a better position to understand what data about them are collected and how they are used."

The report proposes a taxonomy of different TETs ranging from privacy dashboards, self-extracting information tools, and user supports to seals and logos. Dashboards provide data subjects visibility on the collection and processing of their personal data whereas self-extracting tools do not depend on declarations by service providers and automatically extract the pertinent information. ENISA makes note of browser add-ons such as Lightbeam,[21] TaintDroid,[22] or Mobilitics. TETs like the Tos;Dr[23] and TOSBack[24] tools support website users by evaluating and tracking the evolution of privacy policies.[25] In order to be effective, these TETs need to be trusted by users and designed in a comprehensive manner.

The question of consent is closely linked to the lawfulness of the processing principle. ENISA notes that, "to enable lawful data processing of individuals' personal identifiable information, individuals need to give specific, informed and explicit indication of their intentions."

In a report prepared by the Technology Analysis Division of the Office of the Privacy Commissioner of Canada, one way to ensure trust in privacy policies would be to implement a "data tagging" PET that allows organizations to tag data subject information with their specific preferences. For example, "sticky policies" have recently gained interest and allow organizations to "technically enforce preferences when personal data is shared across multiple parties." In some respects, it's like a cookie except that it is not static in nature; instead it's being attached (hence "sticky") to a set of personal data as it is transferred across different platforms and defining how the personal data are to be used. Sticky policies, for example, can be found in the PrimeLife Policy Language (PPL), which is an attempt to develop an

Despite the notable press and fines for privacy deficiencies, Facebook offers an interesting example of how PETs can take data subject control to the next level. In August 2019, Facebook launched a worldwide service that allowed its users to track and delete their personal data sent by websites, online services, and apps to Facebook.

industry standard language for designing such "sticky policies."[26]

Beyond consent: Data tracking

Data tracking allows data subjects to manage their consent and control how their personal data are shared. It allows data subjects to see their personal data's digital trail, including who is processing it all.[27] Such technology is part of the privacy by default principle because the settings limit the personal data sharing to only processing purposes. This approach is very much aligned with GDPR, which "requires organizations to give individuals a range of prescribed information about the processing of their personal data, subject to certain exceptions."[28]

Despite the notable press and fines for privacy deficiencies, Facebook offers an interesting example of how PETs can take data subject control to the next level. In August 2019, Facebook launched a worldwide service that allowed its users to track and delete their personal data sent by websites, online services, and apps to Facebook. This technology allows users to track their data and control the transfers by blocking them in the future or deleting the already transferred data.[29] According to Facebook CEO Mark Zuckerberg this new tool "marks a new level of transparency and control."[30]

Controlling access: From systems to user

This is one area that data controllers have been able to manage successfully, largely since this requirement is synonymous with IT security best practices, industry standards, and good business sense. This requires establishing internal processes to limit who has access to certain information. While the case for data controllers to be able to effectively control data is more or less understood, a more complex question is how to empower data subjects to control their own personal data. In the aforementioned ENISA report, special PET tools known as Intervenability-Enhancing Techniques (IET) can answer this question.

These technologies provide "the possibility to intervene and encompasses control" by the user.[31] IETs are not only pure technologies but can also be considered as organizational processes and measures. These are closely linked to consent management and data tracking functions and as such fall generally within the category of TETs and PDS.

For the Canadian Technology Analysis Division, PETs allow control over data by limiting "the type or quantity of information" disclosed to third parties.[32] These technologies are sometimes called Selective Disclosure Techniques or Technologies (SDT). With these technologies attribute-based credentials (ABC) limit the information disclosed in transactions. The division mentions two ABCs: Microsoft's UProve and IBM's Identity Mixer.

The report also mentions two other technologies that give data subjects better control over their personal data. Firstly, self-sovereign identity placing the user "at the centre of the administration of their identity." One example of software containing this technology is UPort.[33] And secondly, Personal Information Management Systems (PIMS) give data subjects the ability to "decide with whom they share, … for what purposes, and for how long." Such a technique can take the form of personal data dashboards and PDS. The report also mentions specific software giving control over data, for example TACYT (listing threats to mobile apps).[34]

Two additional technologies are worth mentioning: the P3P protocol[35] designed by the World Wide Web Consortium, which gives "browsing users more control [over] their personal information" by "allowing web servers to declare their privacy policies (…) [and] enabling users to negotiate the release of their details."[36] In addition, in 2011 the United Kingdom developed midata tool allowing citizens to control the data about them.

Protecting privacy

Data minimization

According to this principle, only the data that are specifically needed for each specific purpose shall be processed. Implementing the notion of data minimization has proven difficult in practice, for the simple reason that companies are instinctively inclined to collect more data than less. But the challenge is to have a static mindset and only collect the minimal amount of data required for the defined process at a given point in time.[37] This is closely linked to privacy by default.[38] From an accountability perspective, this approach requires that only data are collected that are specifically required while creating less risk for the data controller.

Innovative PETs now offer organizations solutions to ensure minimal data collection. ENISA mentions the now widely used technology of single-sign-on (SSO), which allows users to use

a single identity and hence minimal personal data as part of company-wide access to various corporate tools. One noteworthy example of a SSO standard is the one used by US educational institutions under the name of Shibboleth.[39] ENISA explains that the SSO approach is particularly privacy-friendly, citing the example of an "on-line library providing material to members of the university, [that] may not need to know the exact user but merely [his] university membership status."[40]

The Canadian Technology Analysis Division includes in this category of PETs "websites that deliberately choose not to collect and store personal information such as search terms, search history, IP addresses" like DuckDuckGo,[41] IXquick (now Startpage),[42] Disconnect,[43] or other tools designed to delete browser histories like Privacy Eraser. Finally, the report also mentions PETs that allow temporary communications like Snapchat[44] that auto-delete after a certain time period.

In its report on the role of PETs in data analysis, the Royal Society presents two PETs that have applicability regarding the data minimization principle. The first one is homomorphic encryption: a "form of encryption that allows certain computations on encrypted data, generating an encrypted result which, when decrypted, matches the result of the same operations performed on the data before encryption."[45] Since this PET can be used to compute some data without revealing the content of the data (which is encrypted), the volume of potentially outsourced data is limited. The second one is differential privacy security (discussed in more detail below), which means that "when a dataset or result is released, it should not give much more information about a particular individual than if that individual had not been included in the dataset."[46]

The Enterprise Privacy Group in its report from 2008 mentions the acquisition by Microsoft of Credentica's U-Prove technology[47] which is a user-centric identity management system "enabling users to enforce data minimization." This allows data subjects to limit the released data and has been especially pertinent in the areas of cross-domain enterprise identity and access management, e-government SSO and data sharing, electronic health records, anonymous electronic voting,

Notable fines and the logic behind them

Some interesting examples of how companies failed to implement privacy by design and the sanctions that followed are worth noting. On Nov. 26, 2019, the CNIL imposed a €500,000 administrative fine on Futura Internationale, a home insulation company, for failing to protect the rights of data subjects and for collecting and processing excessive personal data not related to the stated business purpose. In addition to the fine, the CNIL also went as far as to publish the sanction on its website (reminiscent of US regulators' approach to naming and shaming).[9]

Other regulators are unsure of how much to fine companies for GDPR non-compliance. During their twice-annual meeting, known as the *Datenschutzkonferenz* (DSK), the German Supervisory Authorities issued guidelines on Oct. 14, 2019 on how to assess sanctions for violating GDPR.[10] Regulators consider turnover an appropriate factor to ensure that fines are proportionate to the economic activities of an organization. The procedure involves an assessment of the size of the company followed by an analysis of average financial data and market factors that results in an appropriate fine to impose. This guidance has spurred more frequent and higher fines.

The German federal data protection Supervisory Authority *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* (BfDI) imposed a roughly €9.5M administrative fine on the 1&1 Telecom GmbH company on Dec. 9, 2019 for non-compliance with Article 32 of the GDPR. The authority noted that the company failed to implement technical and organizational measures (*technisch-organisatorischen Massnahmen*) to prevent third parties from having undue access to client data using the customer service.[11]

The Austrian Supervisory Authority *Datenschutzbehörde* (DSB) imposed on Aug. 12, 2019 a €50,000 administrative fine (*Gesamtstrafe*) on a medical structure that failed to comply with the GDPR's Data Protection Impact Assessment (DPIA) requirement of Article 35. The DSB underlined that the organization's argument of claiming to be misinformed on GDPR provisions was not legally valid.[12]

On Sept. 17, 2019, the Belgian *Autorité de protection des données* (APD) imposed a €10,000 administrative fine after identifying violations of the GDPR principles of data minimization (Art. 5, GDPR), lawfulness of processing (Art. 6, GDPR), and the right to receive information (Art. 13, GDPR). In this case, the data controller used the on-line identification of clients to create loyalty cards. Clients were not able to receive loyalty cards if they refused to "opt-in" to the use of their personal data.[13]

As is evident in the above examples, effective implementation of privacy by design and by default measures would most likely have allowed these organizations to avoid sanctions and scrutiny altogether.

PETs offering anonymity or even pseudonymization are fundamental to privacy by design. Article 25 (1) of the GDPR49 highlights pseudonymization serving as an appropriate technical and organizational measure to implement privacy principles and comply with privacy by design.

policy-based digital rights management, social networking data portability, and electronic payments.[48]

The (elusive) Holy Grail of anonymity

PETs offering anonymity or even pseudonymization are fundamental to privacy by design. Article 25 (1) of the GDPR[49] highlights pseudonymization serving as an appropriate technical and organizational measure to implement privacy principles and comply with privacy by design.

Anonymity can be invoked for many scenarios but is most often cited with ensuring secure private communications. But while such communications are protected by end-to-end encryption (i.e., underlying transmission is protected), the individuals communicating can still be identified via so-called metadata. ENISA's report highlights this risk: "End-to-end encryption may be used to protect the content of communications, but leaves meta-data exposed to third-parties."[50] As a result (and to the benefit of law enforcement, government intelligence, or malicious third parties), the data on who is talking, time and volume of messages, location, etc. are readily identifiable.

Different technologies are mentioned in the ENISA report to help ensure anonymity and include technology solutions such as single proxies (i.e., using an intermediate proxy service to hide the source IP address) and VPNs (i.e., virtual private networks that operate as a secure subset from the open internet), which are the "simplest means" for protection. PETs are slowly adapting to offer solutions for such techniques.

"Onion routing" (i.e., encapsulating messages in layers of encryption) can also be used to carry communications relying on multiple relays, the Tor service being the most well known.[51] While these technologies can be effective, it is still possible to use classical statistical analysis to unmask identity.[52] To prevent against such risk, technologies such as mix-networks like mixmaster or mixminion are effective. They employ advanced and relatively complex transmission techniques. Other techniques to ensure anonymity include broadcast schemes that work by broadcasting messages to "everyone in a group without any destination of the recipient." While effective in theory, this anonymity technique has its shortcomings in terms of practicality and costs as groups grow in size.

The Canadian Technology Division also highlights techniques such as pseudonymization, anonymizers, disposable/one-time email addresses, random IP addresses — all of which can be applied to email, web browsing, peer-to-peer (P2P) networking, VoIP, chat, and instant messaging, among others.[53] These techniques each offer pros and cons for the elusive quest for true anonymity.

Truly understanding the prospects of genuine anonymity requires some understanding of the mathematical mechanics of differential privacy, which implies trade-offs as measured against setting a value known as epsilon. This approach allows the public to benefit from information derived from a dataset while safeguarding information on the individuals contained in that dataset. The variable epsilon can be modulated to determine just how difficult it would be to identify an individual in the dataset, which has a direct correlation on the utility of the underlying dataset.[54] Differential privacy is at the forefront when it comes to anonymization, and PETs are still evolving to address this developing area.

How to choose the right PET

As illustrated earlier, PETs can be highly technical in nature and not very intuitive when it comes to the desired value of privacy by design and by default. PETs have varying maturity and readiness levels, meaning that not all of them are ready to be deployed in practice on a large scale.[55] To help focus selection of PETs different criteria can be used to assess which PET is best suited for a given organization, like the degree of protection offered by the PET or the proportion of investment likely to be required to integrate a PET.[56] Choosing the right PET(s) requires some serious analysis and of course input from IT specialists to assist with making the right choice for the organization.

Future prospects for PETs

As anyone who has seriously used innovative and cutting-edge technology within a global organization, the line between the technology driving the organization as opposed to the organization driving the technology is a fine one. Organizations have an inherent penchant for adopting technology to solve organizational issues that should be addressed before expecting a technology enabler to solve a compliance or business issue.

And that is exactly what PETs are: technology enablers that can act as levers to drive privacy by design and by default. But as Facebook learned, adopting the most advanced PET — allowing for best-in-practice user control and consent management — has not prevented regulatory scrutiny and sanctions. With this said, the future of PETs is bright. Privacy professionals are increasingly nurturing partnerships with IT departments, which are best

placed to identify and evaluate which tools are best suited to meet privacy by design and by default requirements.

And while there is no one perfect PET solution nor recommendation that stands out above the others mentioned in this article, PETs will increasingly play a role in privacy programs that are serious about privacy by design and by default. To make the right choice, organizations will first have to understand their data flows, risk profile, and relationship with third parties to determine which PETs (if any) are most relevant. Organizations with a focus on data protection compliance continue to welcome PETs with open arms for the simple reason that they can assist with/ensure privacy compliance in a cost effective way.

The landscape is therefore set for specialized technology vendors to continue to develop innovative solutions that address the obligations imposed on data controllers to be GDPR compliant. But remember, these solutions are only effective if used smartly within an organization that understands PETs are simply enablers and not substitutes for an effective privacy governance program. **ACC**

NOTES

1 Article 25 (1), GDPR.
2 Opinion 5/2018, Preliminary Opinion on privacy by design, EDPS.
3 *www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf.*
4 *www.ipc.on.ca/wp-content/uploads/2018/01/pbd.pdf.*
5 Opinion 5/2018, Preliminary Opinion on privacy by design, EDPB.
6 *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/.*
7 Article 83, GDPR.
8 2018 Annual Report, CNIL.
9 *www.cnil.fr/fr/futura-internationale-sanction-de-500-000-euros-pour-demarchage-telephonique-illegal.*
10 *Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bussgeldzumessung in Verfahren gegen Unternehmen*, DSK, 2019.
11 *www.bfdi.bund.de/SiteGlobals/Modules/Buehne/DE/Startseite/Pressemitteilung_Link/HP_Text_Pressemitteilung.html*
12 *Die Verantwortlichkeit zur Einhaltung der sich aus der DSGVO ergebenden Pflichten, ignorantia iuris non excusat - Unwissenheit schützt nicht vor Strafe*, DSB Newsletter, 4/2019.
13 Chambre contentieuse, 17 septembre 2019, DOS-2018-04470, *Plainte pour l'utilisation de la carte d'identité pour la création d'une carte de fidélité.*
14 Opinion 5/2018, Preliminary Opinion on privacy by design, EDPB.
15 *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/*
16 *Privacy by design, An Overview of Privacy Enhancing Technologies,* Enterprise Privacy Group, 26th November 2008.
17 *PETs Controls Matrix report*, ENISA, Chapter 4.
18 Article 6, GDPR.
19 *Privacy and Data Protection by Design – from policy to engineering*, ENISA, December 2014.
20 *Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis*, The Royal Society, March 2019.
21 *https://en.wikipedia.org/wiki/Lightbeam_(software).*
22 */www.appanalysis.org.*
23 *https://tosdr.org.*
24 *https://tosback.org.*
25 *Privacy and Data Protection by Design – from policy to engineering*, ENISA, December 2014.
26 *Privacy Enhancing Technologies, A Review of Tools and Techniques*, Report prepared by the Technology Analysis Division of the Office of the Privacy Commissioner of Canada, November 2017.
27 *Privacy Enhancing Technologies, A Review of Tools and Techniques*, Report prepared by the Technology Analysis Division of the Office of the Privacy Commissioner of Canada, November 2017.
28 *European Union General Data Protection Regulation 2016*, Privacy Commissioner for Personal Date, Hong Kong.

To make the right choice, organizations will first have to understand their data flows, risk profile, and relationship with third parties to determine which PETs (if any) are most relevant.

29 *www.lemonde.fr/pixels article/2020/01/29/activite-en-dehors-de-facebook-comment-voir-et-supprimer-les-donnees-envoyees-a-facebok-par-des-sites-tiers_6027688_4408996.html.*
30 *https://about.fb.com/news/2020/01/data-privacy-day-2020/.*
31 *Privacy and Data Protection by Design* – from policy to engineering, ENISA, December 2014.
32 *Privacy Enhancing Technologies, A Review of Tools and Techniques*, Report prepared by the Technology Analysis Division of the Office of the Privacy Commissioner of Canada, November 2017.
33 *www.uport.me.*
34 *www.elevenpaths.com/technology/tacyt/index.html.*
35 *www.w3.org/P3P/.*
36 *Privacy by design, An Overview of Privacy Enhancing Technologies*, Enterprise Privacy Group, 26th November 2008.
37 Guidelines 4/2019 on Article 25, Data Protection by Design and by Default, EDPB.
38 *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/.*
39 *www.shibboleth.net.*
40 *Privacy and Data Protection by Design – from policy to engineering*, ENISA, December 2014.
41 *https://duckduckgo.com.*
42 *www.startpage.com/en*
43 *https://disconnect.me.*
44 *Privacy Enhancing Technologies, A Review of Tools and Techniques*, Report prepared by the Technology Analysis Division of the Office of the Privacy Commissioner of Canada, November 2017.
45 *Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis*, The Royal Society, March 2019.
46 Ibid.
47 *www.credentica.com.*
48 *Privacy by design, An Overview of Privacy Enhancing Technologies*, Enterprise Privacy Group, 26th November 2008.
49 Article 25, GDPR.
50 *Privacy and Data Protection by Design – from policy to engineering*, ENISA, December 2014.
51 *www.torproject.org.*
52 *Privacy and Data Protection by Design – from policy to engineering*, ENISA, December 2014.
53 *Privacy Enhancing Technologies, A Review of Tools and Techniques*, Report prepared by the Technology Analysis Division of the Office of the Privacy Commissioner of Canada, November 2017.
54 *Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis*, The Royal Society, March 2019.
55 *Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies*, ENISA Report, 2016.
56 *Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis*, The Royal Society, March 2019.

ACC EXTRAS ON... Privacy technology

ACC Docket

How In-house Leaders Can Use Technology to Better Prepare for the Next Crisis (July 2020). *accdocket.com/articles/how-in-house-leaders-technology-risk-mitigation.cfm*

Turning Consumer Privacy Expectations into Trust (Dec. 2019). *accdocket.com/articles/resource.cfm?show=1505265*

Tips & Insights: In the Heart of Technology (Oct. 2019). *accdocket.com/articles/tips-insights-in-the-heart-of-technology.cfm*

ACC HAS MORE MATERIAL ON THIS SUBJECT ON OUR WEBSITE. VISIT *WWW.ACC.COM*, WHERE YOU CAN BROWSE OUR RESOURCES BY PRACTICE AREA OR SEARCH BY KEYWORD.

NOW AVAILABLE!

ACC Foundation
Association of Corporate Counsel

2020 STATE OF CYBERSECURITY REPORT

AN IN-HOUSE PERSPECTIVE

586 DEPARTMENTS

20 INDUSTRIES

36 COUNTRIES

IN TODAY'S ALL-VIRTUAL WORLD, THE LEGAL DEPARTMENT'S ROLE IN CYBERSECURITY HAS BECOME MORE IMPORTANT THAN EVER.

With multiple aspects of business being conducted online, cybersecurity is naturally a topic at the forefront of people's minds. The ACC Foundation 2020 State of Cybersecurity Report expands on in-house counsel's growing role in companies' cybersecurity functions, as well as dives into legal's impact on and involvement in cybersecurity policies, practices, and risk management.

BE INFORMED. DOWNLOAD THE KEY FINDINGS FOR FREE OR PURCHASE THE REPORT AT

acc.com/cyber2020