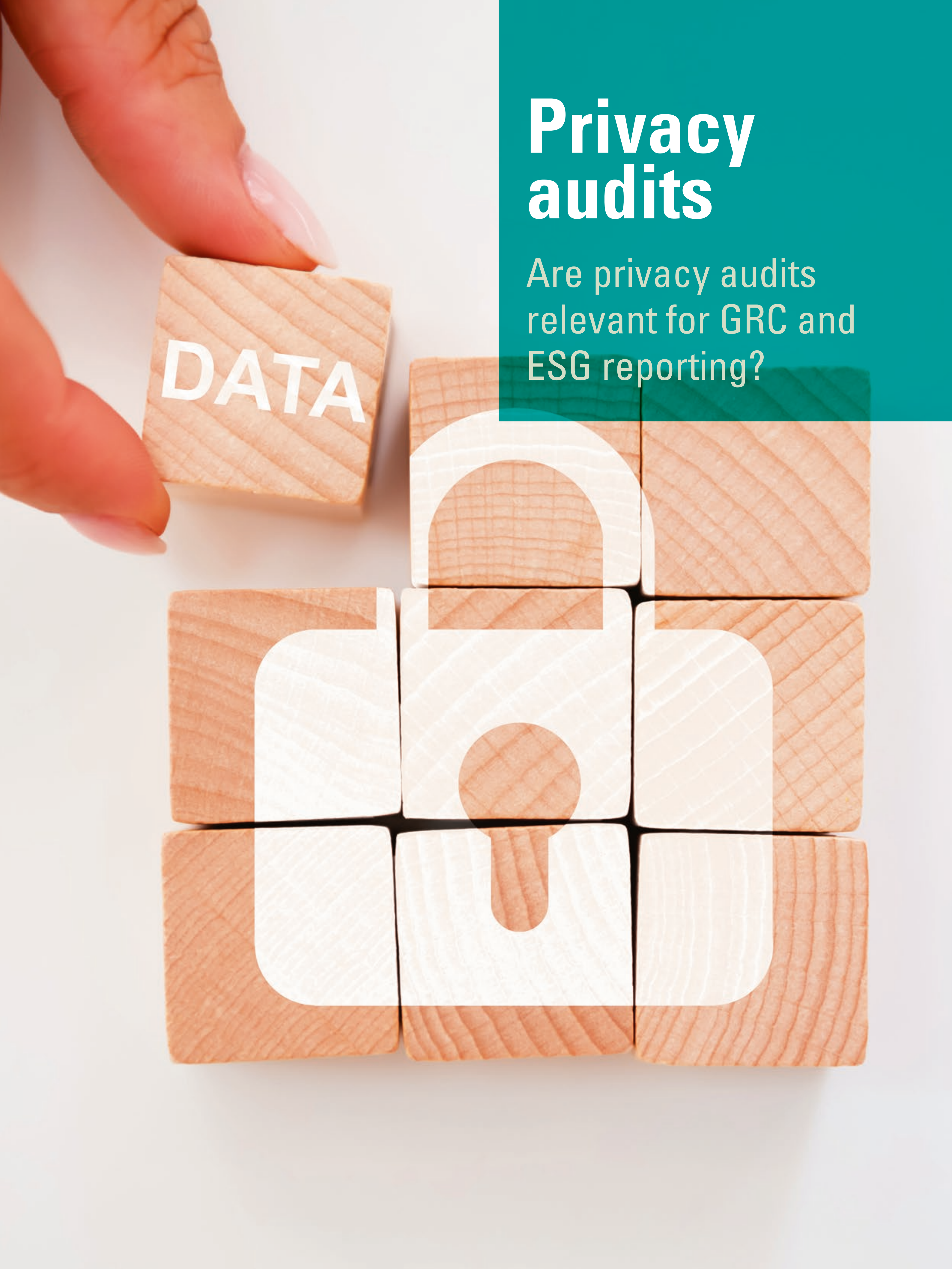
# Privacy audits

Are privacy audits relevant for GRC and ESG reporting?



**The importance of data privacy has increased incredibly in the last couple of years. With the introduction of the General Data Protection Regulation (GDPR), the importance of data privacy has increased even more. Data privacy is an important management aspect and contributes to sustainable investments. It should therefore take a prominent role in GRC efforts and ESG reporting. This article discusses the options to perform privacy audits and the relevancy of the outcomes.**

Maryam Amaador
is a senior consultant at KPMG IT Assurance & Advisory.

drs. Henk Hendriks RE CISA
is a senior information risk controller at Menzis.

## INTRODUCTION

In recent years, there have been various developments with regard to data privacy. These developments, and especially the introduction of the General Data Protection Regulation (GDPR), forced organizations to become more aware of the way they process personal data. However, not just organizations have been confronted with these developments, individuals who entrust organizations with their data have also become more aware of the way their personal data is processed. Therefore, the need to demonstrate compliance with data privacy laws, regulations and other data privacy requirements has increased among organizations.

Since data privacy is an important management aspect and contributes to sustainable investments, it has taken a prominent role in Governance, Risk management & Compliance (GRC) efforts and Environmental, Social & Governance (ESG) reporting. GRC and ESG challenges organizations to approach the way they are dealing with personal data from different angels and the way they report on their performed efforts. However, because of the complexity of privacy laws and regulations and a lack of awareness, it seems to be quite a challenging task for organizations to demonstrate the adequacy of their privacy implementation. It seems that a lot can be gained when determining whether controls are suitably applied in this regard, since there are no straightforward methods that could be applied to provide insight. The poor state of awareness and knowledge on this topic makes this even more complicated.

This article explains the criticality of GDPR in obtaining compliance, followed by a description of the various ways in which privacy compliance reporting can be performed. In addition, the role of privacy audits, their value, and the relationship of privacy audits to GRC & ESG is explained, prior to providing some closing thoughts on the development of the sector. The key question in this article is whether privacy audits are relevant for GRC & ESG.

## CRITICALITY OF THE GDPR IN OBTAINING COMPLIANCY

Although the GDPR has already been implemented in May 2018, it is still a huge challenge for organizations to cope with. This privacy regulation has not only resulted in the European Commission requiring organizations to prove their level of compliance, but it has also increased the interest from individuals on how their personal data is processed by organizations. The most important principles of the GDPR, as listed in article 5 are:

1. Lawfulness, Fairness, and Transparency
2. Limitations on Purposes of Collection, Processing & Storage
3. Data Minimization
4. Accuracy of Data
5. Data Storage Limits and
6. Integrity and Confidentiality

The rights that individuals have as data subjects are listed in Chapter 3 of the GDPR and are translated into requirements that should be met by organizations, such as:

1. The right to be informed – organizations should be able to inform data subjects about how their data is collected, processed, stored (incl. for how long) and whether data is shared with other (third) parties.
2. The right to access – organizations should be able to provide data subjects access to their data and give them insight in what personal data is processed by the organizations in question.

3. The right to rectification – organizations must rectify personal data of subjects in case it is incorrect.
4. The right to erasure/the right to be forgotten – in certain cases, such as when the data is processed unlawfully, the individual has the right to be forgotten which means that all personal data of the individual must be deleted by the data processor.
5. The right to restrict processing – under certain circumstances, for example, when doubts arise about the accuracy of the data, the processing of personal data could be restricted by the data subject.

A starting point for any organization to determine whether and which privacy requirements are applicable to the organization is a clear view of the incoming and outcoming flows of data and the way the data is processed within and outside the organization. In case personal data is processed, an organization should have a processing register. Personal data hereby being defined as any data which can be related to natural persons. In addition, the organization should perform Data Privacy Impact Assessments (DPIAs) for projects that implement new information systems to process sensitive personal data and a high degree of privacy protection is needed.

The obligation to possess a data processing register and the obligation to set up DPIAs, ensure that the basic principles that are required by the privacy regulation for the processing of personal data (elaborated in Chapter 2 of the GDPR) and privacy control have the right scope. Furthermore, these principles ensure that processing of personal data by an organization is done in a legitimate, fair and transparent way. Organizations should hereby bear in mind that processing personal data is limited to the purpose for which the data has been obtained. All personal data that is requested should be linkable to the initial purpose. The latter has to do with data minimization, which is also one of the basic principles of the GDPR. Regarding the storage of data, organizations should ensure that data is no longer stored than is necessary. The personal data itself should also be accurate and must be handled with integrity and confidentiality.

Organizations are held accountable by the GDRP for demonstrating their compliance with applicable privacy regulations. The role of the Data Protection Officer (DPO) has increased considerably in this regard. The DPO is often seen as the first point of contact for data privacy within an organization. It is even mandatory to appoint a DPO in case the organization is a public authority or body. DPOs are appointed to fulfill several tasks such as informing and advising management and employees about data privacy regulations, monitor compliance with the GDPR and increase awareness with regard to data privacy by for example, introducing mandatory privacy awareness training programs.

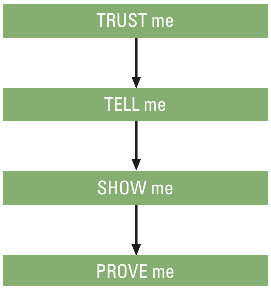
Demonstration of compliance with privacy regulations could be quite challenging for organizations and especially for DPOs. Complying with privacy regulations has been outlined in article 42 of the GDPR. However, practice has shown that demonstrating compliance is more complex than is described in this article. At this moment the Dutch Authority of Personal Data (Autoriteit Persoonsgegevens), the Dutch accreditation council (Raad voor Accreditatie) and other regulators have not yet come to a practical approach for issuing certificates to organizations that meet the requirements, due to the elusive nature of the law article. Besides the certification approach foreseen in the GDPR, there are different approaches in the market which organizations can use to report on their privacy compliance. In the next section some of these reporting approaches are elaborated on.

## REPORTING ON PRIVACY COMPLIANCE

There are different ways in which organizations can report on privacy. Of course there are self-assessments and advisory-based privacy reporting. These ways of reporting on privacy are mostly unstructured and the conclusions subjective, however. The reports therefore make it difficult to benchmark organizations against each other. To make privacy compliance more comparable and the results less questionable, there are broadly speaking two ways of more structured reporting in the Netherlands. These ways are reporting based on privacy assurance and reporting based on privacy certification. They are further explained in the following paragraphs of this section.

### A. Reporting based on privacy assurance

Assurance engagements can be defined as assignments in which auditors give an independent third-party statement (“opinion”) on objects by testing suitable criteria. Assurance engagements are meant to instill confidence in the intended users. These engagements originate in the financial audit sector. How these engagements should be performed and reported are predefined by internationally accepted “Standaarden” (standards) respectively “Richtlijnen” (guidelines) and are propagated by the NBA and NOREA.[1]



[1] The NBA and NOREA are the Dutch bodies for financial respectively IT auditing.

As part of assurance engagements, controls are tested using auditing techniques consisting of the Test of Design (ToD) and/or Test of operating Effectiveness (ToE). Based on the results of controls testing, an opinion is given on the research objects. This opinion can be either qualified, unqualified, abstaining from judgment, or qualified with limitation. The most commonly used assurance "Standaarden" and "Richtlijnen" in the Netherlands to report on privacy are: ISAE 3000, SOC1 and SOC2. ISAE3000 is a generic standard for assurance on non-financial information. SOC1 is meant to report relevant non-financial control information for financial statement analysis purposes and SOC2 is set up for IT organizations that require assurance regarding security, availability, process integrity, confidentiality and privacy related controls. Assignments based on ISAE3000, SOC1 and SOC2 can lead to opinions on privacy control. The criteria chosen to be in scope as part of an ISAE3000 or SOC1 engagement can be chosen freely as long as the choice leads to a cohesive, clear and a usable result. The criteria for SOC2 are prescribed, although extension is possible.

NOREA gives organizations the possibility to obtain a Privacy Audit Proof quality mark for individual or multiple processing activities of personal data or for an entire organization ([NORE21]). This mark can be obtained based on a "ISAE3000" or "SOC2" privacy assurance report with an unqualified opinion. The NOREA Taskforce Privacy has set up terms in which guidelines for performing privacy assurance engagements and obtaining the Privacy Audit Proof quality mark. One of the conditions for this quality mark is the usage of the NOREA Privacy Control Framework (PCF) as a set of criteria, in case of the usage of the ISAE3000, or the usage of the criteria elaborated in the privacy paragraph of an SOC2-assurance report. The Privacy Audit Proof quality mark can be obtained by either controllers or processors. After handing over an unqualified assurance report and giving relevant information, NOREA gives permission to the organization that is being successfully audited to use this mark for one year, under certain conditions.

The extent to which an opinion on privacy control resulting from an assurance engagement is the same as an opinion on privacy compliance depends on the criteria in scope of the assurance engagement. An opinion on privacy controls, although a good indicator, can however never be seen as an all-encompassing compliance statement. Due to the fact that the GDPR is ambiguous and the selection of controls in scope requires interpretation, an objective opinion on compliance by financial or IT auditors is not possible.

Demonstration of compliance with privacy regulations can be quite challenging for organizations

### B. Reporting based on privacy certification

Certification originates from quality control purposes. To be eligible for a certification, an independent, accredited party should assess whether the management system of the concerned organization meets all requirements of the standard. Certification audits are meant to making products and services comparable. In addition, the strive for continuous improvement is an important part of these audits.

In general, the most commonly used certifications in the Netherlands are those originating from the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) ([ISO21]). Examples of ISO/IEC-standards are the ISO/IEC 27001 (information security management), the ISO/IEC 27002 (information security), the ISO/IEC 27018 Information technology) and the ISO/IEC 29100 (for public cloud computing). In addition, the ISO27701 has been introduced in August 2019 as an extension of ISO27001. This standard focuses on the privacy information management system (PIMS). This particular standard assists organizations to establish systems to support compliance with the European Union General Data Protection Regulation (GDPR) and other data privacy requirements but as a global standard it is not GDPR specific.

Other privacy certification standards are for example the BS10012, European Privacy Seal (also named EuroPrise), the Europrivacy GDPR certification and private initiatives, like certification on the Data Pro Code ([NLdi21]). BS10012, as the British Standard on PIMS, is mostly replaced by the ISO27701. EuroPrise provides certifications that demonstrate that for example IT products and IT-based services, comply with the European data protection laws ([EuPr21]). Europrivacy GDPR certification, as is stated on their website, "provides a state-of-the-art methodology to certify the conformity of all sorts of data

| Aspects | Privacy Assurance (based on 3000) | ISO 27001/27701 Certification |
|---|---|---|
| **Specific target audience** (closed user group) | ✓ | ✗ |
| **Standard set of criteria** | ✓ (due to NOREA PCF) | ✓ |
| **Client/sector/IT-specific criteria** | ✓ | ✗ |
| **Test of Management System** | ✗ / ✓ | ✓ |
| **Test of design** (Documentation audit) | ✓ | ✓ |
| **Test of Operational Effectiveness** (Implementation audit) | ✓ | ✗ |
| **Standard reporting** | ✓ (due to NOREA PCF) | ✓ |
| **Reporting of exceptions** | ✓ | ✗ |
| **Provide (reasonable) assurance** | ✓ | ✗ |

**Figure 1.** Comparison privacy assurance versus privacy certification (based on [Zwin21]).

processing with the GDPR". In the Netherlands, NL Digital, as an organization of ICT companies, has developed the Data Pro Code. This Code specifies the requirements of the GDPR for data processors. Due to their specific nature the Europrivacy GDPR certification and certification on the Data Pro Code are less commonly used in The Netherlands.

### C. Privacy assurance versus privacy certification

The main difference between privacy assurance and certification is that assurance is more assignment-specific and in-depth. This is illustrated in Figure 1. In this figure, the main differences between privacy assurance based on ISAE/COS or Directive 3000 and Certification according to ISO 27701 are summarized.

Since the privacy reporting business hasn't matured yet, privacy assurance and privacy certification can coexist and have their own benefits. Organizations that want to report on privacy should choose the way that suits their needs, which is dependent on their level of maturity for instance.

## PRIVACY AUDITS

Although a lot of knowledge and experience is available, performing an audit is an intensive process. This is especially the case for privacy audits. Since personal data is cross sectional, a separate area and not tangible, privacy audits are considered to be even more difficult.

This section describes typical aspects of privacy audits. As a model for describing these aspects, a privacy audit is considered to follow the phases shown in Figure 2.

In general, the privacy audit phases look like the phases of "regular" audits. There are a few differences, however. One of the most important differences between regular and privacy audits is the determination of the scope, which is more difficult for privacy audits. A clear view of the incoming and outcoming flows of data and the way the data is processed within and outside the organization is a good starting point for privacy related efforts, and therefore also for scope determination. The processing register and DPIAs are other "anchors" that are useful. Data flows and the processing register list what data is processed in what system and which part can be considered personal data. DPIAs can provide further insight into the division of responsibilities, sensitivity of the data, applicable laws and relevant threats and vulnerabilities. Although all the aforementioned can help, there are still a few problems to be solved. The most important of these are the existence of unstructured data and the effects of working in information supply chains.

**Figure 2.** Privacy audit phases.

Phase 1 – Determine scope & approach

Phase 2 – Identify data processing & data flows

Phase 3 – Determine applicable legislation/regulation & (sector) requirements

Phase 4 – Perform privacy audit fieldwork

Phase 5 – Identify privacy gaps/risks & recommend remediation

Phase 6 – Reporting & follow-up

Phase 7 – Formal privacy assurance or certification

- Unstructured personal data is data which is not stored in dedicated information systems. Examples of this type of data is personal data stored in Word or Excel files on hard disks or on server folders used in the office automation, such as personal data messages in mailboxes or personal data in physical files. Due to the unstructured character, scope determination is difficult by nature. Possible solutions for these situations can be found in tools which scan for files containing keywords which indicate personal data, like "Mr.", "Mrs." or "street". A more structural solution can be found in data cleansing as part of archiving routines and "privacy by design" and "privacy by default" aspects of system adjustments or implementations. Whereas scanning is diverted to point solutions, archiving and system adjustments or implementations can help find a more structural solution.
- Working in information supply chains leads to the problem that the division of responsibilities among involved parties is not always clear. In case of outsourcing relations, processing agreements can help clarify the relationships between what can be considered the processor and the controller. Whereas the relationships in these relatively simple chains are mostly straightforward, less simple chains like in Dutch healthcare or justice systems lead to more difficult puzzles. Although some clarification can be given in the public sector due to the existence of "national key registers" (in Dutch: "Basisregisters"), most of the involved relationships can best be considered as co-processor relationships, in which there are joint responsibilities. These relationships should be clarified one by one. In addition to co-processor relationships, there are those relationships in which many processor tasks lead to what can be considered controller tasks, due to the unique collection of personal data. This situation leads to a whole new view on the scoping discussion, with accompanying challenges.

Other difficulties performing a privacy audit arise from the Schrems-II ruling. As a result of this ruling, processing of personal data of European citizens under the so-called Privacy Shield agreement in the United States is considered to be illegal. Since data access is also data processing, the use of US cloud providers is to be considered illegal. Although there are solutions being specified like new contractual clauses and data location indicators, there is no entirely privacy-compliant solution available yet. Considering that the US secret service organizations are not bound to any privacy clauses and since European citizens are not allowed on the American privacy oversight board, there is still a leak.

Testing privacy controls is not simple either. Of course there are standard privacy control frameworks and the largest part of these frameworks consists of security controls and PIMS. There is a lot of experience with testing these. Testing controls which guard the rights of the data subjects, like the rights to be informed, access and rectification is more difficult, however. This difficulty arises from the fact that these controls are not always straightforward and testing these requires interpretation of policies and juridical knowledge. These difficulties can of course be overcome by making it explicit that an audit on privacy cannot be considered a legal assessment. This disclaimer is, however, not helpful in gaining the intended trust.

To improve the chance of successfully testing controls, most privacy audits are preceded by a privacy assessment advisory engagement. These advisory engagements enable the suggestion of improvements to help organizations, whereas audits, especially those devoted to assurance, leave less room to do so.

Reports resulting from privacy audits are mainly dictated by the assurance or certification standards, as described in the preceding section. The standard and resulting report should suit the level of maturity of the object and the trust needed so that maximum effect can be reached.

## ADDED VALUE OF PRIVACY AUDITS

Privacy audits lead to several benefits and added value. In this section the most important are listed.

*Building or restoring confidence* – Like any audit performed for an assurance or certification assignment, a privacy audit is devoted to help build or restore confidence. This is even more so if the privacy audit leads to a quality mark.

*Increasing awareness* – Whether an audit leads to a qualified opinion or not, any audit leads to awareness. The questions raised and evidence gathered make employees aware. Since the relevance of privacy has increased over the past years, a privacy audit can help with prioritizing the subject within the organization as the outcomes could eventually lead to necessary follow-up actions that require the engagement of several employees/departments within the organization.

*Providing an independent perspective* – As mentioned before, privacy is not an easy subject. Therefore, subjectivity and self-interest are common pitfalls. Auditors can help avoid risks related to these pitfalls by independently rationalizing situations.

*Giving advice on better practices* – Auditors are educated to give their opinion, based on the last regulations and standards. Therefore, the auditors' advice is based on better practices. Since privacy is an evolving and immature business, advising on better practices has taken a prominent role in their job and provided services.

*Facilitating compliance discussions* – Last not but not least, although auditors do not give an opinion on compliance, they facilitate compliance discussions inside and outside client organizations, due to their opinion on relevant criteria and controls. In this respect, the auditor can also help in discussions with supervisory boards. Assurance, certification and quality marks are proven assets in relationships with these organizations.

**Client case: Privacy audits at RDW**

A good example of how privacy reporting can be helpful are the privacy audits performed for the Dutch public sector agency that administers motor vehicles and driving licenses "RDW".

RDW is responsible for the licensing of vehicles and vehicle parts, supervision and enforcement, registration, information provision and issuing documents. RDW maintains the "national key registers" ("Basisregisters") of the Dutch government with regard to license plate registration in the "Basis Kentekenregister" (BKR) and the registration of driving licenses in the "Centraal Rijbewijzenregister" (CRB). In addition, RDW is processor of on-street parking data in the "Nationaal Parkeerregister" (NPR) for many Dutch municipalities.

Since there are many interests and there is a lot of personal data being processed, RDW is keen on being transparent on privacy control. KPMG takes care of privacy audits with respect to the abovementioned key registers, BKR, CRB and NPR, as RDW's assurance provider.

Performing these audits, there are the aforementioned challenges with regard to scope. They are dealt with by, amongst others, restricting the scope to the lawfully and contractually confirmed tasks and descriptions in processing registers and PIAs. Furthermore, due to the fact that RDW has a three lines of defense model, with quality control and resulting reports as second line, they have managed to implement privacy controls as listed in the NOREA privacy control framework.

According to the RDW, privacy reports and marks are helpful in, for example, communication to partners in automotive and governmental information supply chains and with supervisory boards. Although there is a lot of innovation in conjunction with, for example, connected and autonomous vehicles, RDW states that they are able to manage accompanying challenges with regard to amongst others privacy protection. If unintentionally something happens like a data breach, RDW is in a good position to give an explanation, supported by audit results.

## POSITION OF PRIVACY AUDITS IN GRC & ESG

ESG measures the sustainable and ethical impact of investments in an organization based on the Environmental, Social and Governance related criteria. Previous events – such as the Facebook privacy scandal in which user data could be accessed without their explicit consent of these users ([RTLN19]) – have shown that data breaches could raise a lot of questions from investors or even result in decreasing share prices. Insufficient GRC efforts regarding data privacy could even lead to doubts about the social responsibility of an organization.

As mentioned in previous sections, there are various ways for organizations to demonstrate their compliance with data privacy regulations. The importance of presenting the way an organization is dealing with data privacy is further emphasized with the introduction of ESG, since it demands privacy to be implemented from an Environmental, Social and Governance point of view as well.

The outcomes of privacy audits could be used as a basis for one of the ESG areas. Privacy audits could provide insights in the extent to which measures are effective and a means to monitor privacy controls. Also, findings that have been identified from a privacy audit could help in ESG as they make organizations aware of the improvements that they have to make to prevent these events in the future to (re)gain the trust of all relevant stakeholders, including (potential) investors.

## CONCLUSION AND FINAL THOUGHTS

Although privacy audits could not provide the ultimate answer on whether organizations comply with all applicable data privacy regulations, it does offer added value.

### References

**[EU16]** European Union (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. *Office Journal of the European Union*. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1635868498095&from=EN

**[EuPr21]** EuroPrise (2021). EuroPrise – the European Privacy Seal for IT Products and IT-Based Services. Retrieved from: https://www.euprivacyseal.com/EPS-en/Home

**[Euro21]** Europrivacy (2021). Europrivacy Certification. Retrieved from: https://www.europrivacy.org

**[ISO21]** ISO (2021). *Standards*. Retrieved from: https://www.iso.org/standards.html

**[Koor13]** Koorn, R., & Stoof, S. (2013). IT-assurance versus IT-certificering. *Compact 2013/2*. Retrieved from: https://www.compact.nl/articles/it-assurance-versus-it-certificering/

**[NLdi21]** NLdigital (2021). *Data Pro Code*. Retrieved from: https://www.nldigital.nl/data-pro-code/

Therefore, the answer to the earlier question on whether privacy audits are relevant for GRC and ESG is, according to us, undoubtfully: "yes, they are!"

Privacy audits cannot provide the ultimate answer to whether organizations comply with all applicable data privacy regulations, however. Using privacy audits, organizations obtain insights into the current state of affairs regarding data privacy management. The outcomes of a privacy audit could also increase further awareness within the organization, as it emphasized the shortcomings that had to be followed up or investigated by the relevant parties within the organization. Next to the benefits that the organization itself will have with the performance of a privacy audit, it facilitates discussions with third parties and supervisory boards when it comes to demonstrating compliance with data privacy regulations, especially when the privacy audit has resulted in a report provided by an independent external privacy auditor. Another advantage of having privacy audits performed is that it lays the foundation for further ESG in which an organization can describe the measures performed to ensure data privacy and the way how progress is monitored. This could explain why sustainable investments are ensured at the organization in question. Privacy audits are difficult, however, since personal data are cross sectional, a separate area and not tangible.

Outsourcing and working in information supply chains are upcoming trends. These trends will offer a lot of opportunities for those who want to make a profit. To gain maximum benefit, the focus of the involved organizations should not only be on offering reliable services; they should also have a clear vision on GRC and ESG aspects. Privacy should be one of these aspects, whereas balanced reporting on all of the aforementioned is the challenge for the future.

Privacy audits are relevant for GRC and ESG

**[NORE21]** NOREA (2021). Privacy Audit Proof: Logo voor de betrouwbare verwerking van persoonsgegevens. Retrieved from: https://www.privacy-audit-proof.nl

**[RTLN19]** RTL Nieuws (2019, July 24). Recordboete voor Facebook van 5 miljard dollar om privacyschandaal. Retrieved from: https://www.rtlnieuws.nl/economie/bedrijven/artikel/4791371/recordboete-facebook-vijf-miljard-toezichthouder

**[Zwin21]** Zwinkels, S., & Koorn, R. (2021). SOC 2 assurance becomes critical for cloud & it service providers. *Compact 2021/1*. Retrieved from: https://www.compact.nl/articles/soc-2-assurance-becomes-critical-for-cloud-it-service-providers/

## About the authors

**Maryam Amaador joined KPMG** in 2018 after obtaining her master's degree in Information Sciences. She is a senior consultant at KPMG's IT Assurance & Advisory department where she focuses on different types of assurance engagements, including privacy assurance. In addition, Maryam also provides IT support to the Financial Statement Audit, in which privacy is taking a more prominent role. Within KPMG, Maryam is part of the privacy assurance taskforce where knowledge is shared regarding the implementation of privacy regulations. In addition to her current job at KPMG, Maryam is currently completing her studies in IT Audit Compliance & Advisory (ITACA) at the Vrije Universiteit Amsterdam.

**Drs. Henk Hendriks RE CISA** is a senior information risk controller at Dutch healthcare insurance company Menzis. He is specialized in, amongst others, internal control and controlling outsourcing and chain relationships. Before his career at Menzis, Henk worked at KPMG IT Assurance & Advisory as a senior manager, mainly active in the public sector and at organizations affiliated with the health industry. At KPMG, he specialized in assurance engagements. In addition to his current job at Menzis, Henk works part time as a lecturer in IT Audit Compliance and Advisory (ITACA) at the Vrije Universiteit of Amsterdam and he is a member of the NOREA Privacy Taskforce.