PICCASO PRIVACY LABS

Explaining the role of privacy in ESG

White Paper

Privacy and data protection is one of the main business risks and yet its linkage to ESG or environmental, social and governance topics, is still a novel concept and in its infancy. It is time to raise awareness on this issue and elevate privacy in sustainability reporting. The aim of this white paper is to explore the role that data privacy plays in ESG, as well as highlights the challenges and opportunities.

IRON MOUNTAIN®

KPMG

PrivacyCulture

Contents

Every company must address this issue

The widespread use of personal data means that data privacy has become a material ESG issue.

The more data a company processes the more this is likely to affect their ESG rating.

There is no doubt that poor privacy is the result of poor environmental, societal and governance practices. At the same time, good privacy and data protection matters is likely to positively impact ESG scores and empower the business. The time has come for all privacy professionals to raise the issue of ESG and data privacy, and in turn help drive change through our organisations, a change for good and all our future generations.

Julia Bonder Le-Berre, Co-chairperson

Graham Thomas, Co-chairperson

Participants:

Julia Bonder Le-Berre, **Iron Mountain**; Graham Thomas, **KPMG UK**; João Barreiro, **Beigene**; Andrea Tota, **Beigene**; Sally Barnard, **Goldman Sachs**; Ian Chown, **BT**; Jimmy Bester, **BT**; Janine Mckelvey, **BT**; Matt Kay, **Metrobank**; Stefano Leucci, **Nexa Center for Internet and Society - Politechnic School of Turin**; Monika Tomczak-Gorlikowska, **Prosus**; Karen Duffy, **Shell**; Mutsa-Washe Mamvura, **PICCASO**; Mukta More, **PICCASO**; Paul Jordan, **PICCASO**; Steve Wright, **PICCASO**; Rahil Zuyaan, **Privacy Culture**; John Watson, **Privacy Culture**;

PICCASO: The "why" of privacy culture practice and ESG

On behalf of PICCASO Privacy Lab, we are delighted to present to you the following insights on the subject of ESG.

PICCASO stands for Privacy, Infosec, Culture, Change & Awareness Societal Organisation. As the name suggests we are a special interest group for professionals and organisations that stand for Privacy, Data Protection and Information Security. PICCASO operates as a not-for-profit entity, steered by dedicated volunteers and industry-leading figures who serve as the PICCASO Advisory Board. Our mission revolves around instilling the 'why' of privacy culture practice and embedding best practices into an organisation's core DNA for enhanced privacy compliance and data strategy.

With over 35 meetings and a collective effort spanning 80 hours, our diverse team of 19 members from various organisations and industries have successfully prepared a comprehensive whitepaper, which is now ready for your review. To ensure a well-structured and collaborative approach, our team members worked in smaller groups, engaging in numerous focused discussions to lay the foundation. On a monthly basis, we convened as a larger group to ensure alignment and steady progress. Throughout this journey, our dedicated chairs provided invaluable feedback, ensuring that our work embodied the highest standards of excellence. To put the finishing touches on our whitepaper, our skilled graphic designer ensured that it is publication-ready for widespread distribution.

1 Why privacy is one of the next key pillars in ESG?

More regulation, more data, more issues

Mounting geopolitical and societal issues, alongside the rapid advent of data-driven disinformation, such as AI deepfakes, the Cambridge Analytica scandal, and the growth of ransomware attacks, have forced governments to act. Now 137 out of 194 countries have legislation in place, or in draft, to secure the protection of data and ensure privacy, according to UNCTAD[1]. Regulations such as the GDPR in the EU, The Data Protection Act in the UK, CCPA in California/U.S., LGPD in Brazil, PIPL in China and recently India's DPDPA are the most well-known.

At the same time, the exponential growth of data usage by businesses has a significant impact, on ESG, particularly the use of generative AI. For instance, the training of the generative AI model ChatGPT-3 used 3.5 million litres of water, according to one study[2]. That is a massive amount, especially considering that the model was trained using efficient U.S. data centres. If this AI model was trained in less efficient Asian data centres, water usage would rise to five million litres. Unless we develop AI systems to better account for its environmental impact, its energy consumption could be greater than that of the entire human workforce by 2025, according to Gartner. [3]

To train Generative AI mode ChatGPT-3:

3.5
MILLION LITRES OF WATER

1.3
GIGAWATT-HOURS

121
U.S. HOUSEHOLDS, POWER FOR ONE YEAR[4]

1. Data Protection and Privacy Legislation Worldwide, United Nations Conference on Trade and Development (UNCTAD)
2. Making AI Less "Thirsty": Uncovering and Addressing the Secret Water Footprint of AI Models, Pengfei Li, Jianyi Yang, Shaolei Ren, UC Riverside (Cornell University, Arvix)
3. Gartner Unveils Top Predictions for IT Organizations and Users, IT Symposium October 18, 2022
4. Large, creative AI models will transform lives and labour, The Economist, April 2023

Evolving digital landscape is driving change

Most businesses now have data at the core of their operations. It is considered a key asset. How they use and protect that data is key to the ESG agenda, as well as customer, employee and societal trust. Data privacy functions also play a key role in ensuring ESG responsibility as they have a remit to ensure that their businesses comply with strong data protection regulations such as GDPR, CCPA, LGPD, PIPL, which positively impact ESG. At the same time, fast developing AI, particularly generative AI and data ethics have a profound effect on data privacy, protection, storage and ultimately ESG. These issues will grow as more organisations digitally transform.

Actions on privacy positively impact ESG

By tackling privacy and data protection issues, as well as adhering to privacy principles, organisations can have a positive impact on ESG and improve their ratings. This can be achieved by focusing on data minimisation and retention, handling data subject requests properly, implementing privacy by design, boosting transparency, understanding data hosting and technology use, as well as implementing training and awareness programmes. However, this is just the beginning. Organisations are also increasingly looking at data hygiene, which is driven by how well a business looks after its data. In the future, this could be aligned more closely to ESG ratings.

Pressure mounting on ESG disclosures

ESG considerations are an integral part of corporate strategy and reporting for many organisations. There is now a greater expectation from investors, consumers and employees for organisations to be more transparent, proactive and accountable for ESG. This is enhanced by the adoption of standards for sustainability disclosures, such as the EU's Corporate Sustainability Reporting Directive (CSRD).

Privacy and ESG are inextricably linked, here's how

There is currently little alignment between privacy, data protection and ESG goals, this makes it challenging for organisations to make the connection, but they are linked:

- **E – Environment:** Exponential growth of data and its storage impacts the environment. More data means a larger carbon footprint. More automation, audits and rationalisation mean less data (whether stored in automated systems or paper records), fewer emails and paper records and a lower carbon footprint.

- **S – Social:** Good data governance gives individuals greater control over their data, drives greater transparency and boosts trust, brand value and personal accountability.

- **G – Governance:** Mature data governance programs, including better handling of data subject rights, strengthens compliance and the approach to risk and control management. It also reduces the scale and materiality of harm in the event of an incident.

Lack of calibration challenges link

Right now, the lack of privacy certifications a business can get makes it difficult to demonstrate the maturity level of an organisation's privacy programmes and in turn influence ESG ratings. As a result, in practice, few rating agencies actually focus on real privacy and data protection issues for ESG scores. Organisations are typically only asked by rating agencies to report on data incidents, customer privacy practices and certification of data management systems. Questions asked by those rating agencies are high level, open-ended, and only form a small part of the overall 'Governance' section. This means that key considerations may be being missed by rating agencies when giving the ESG scores.

Despite significant regulatory developments in privacy and data protection, there's not been an equivalent shift in ESG reporting to mirror this uptick in investment. It means that calibrating privacy and data protection activities, and benchmarking one company against another to generate a true ESG value, is challenging.

Now we have identified privacy as a key pillar in the ESG landscape, in the next chapter there is a need to look at the role that privacy plays in ESG reporting. This raises many issues.

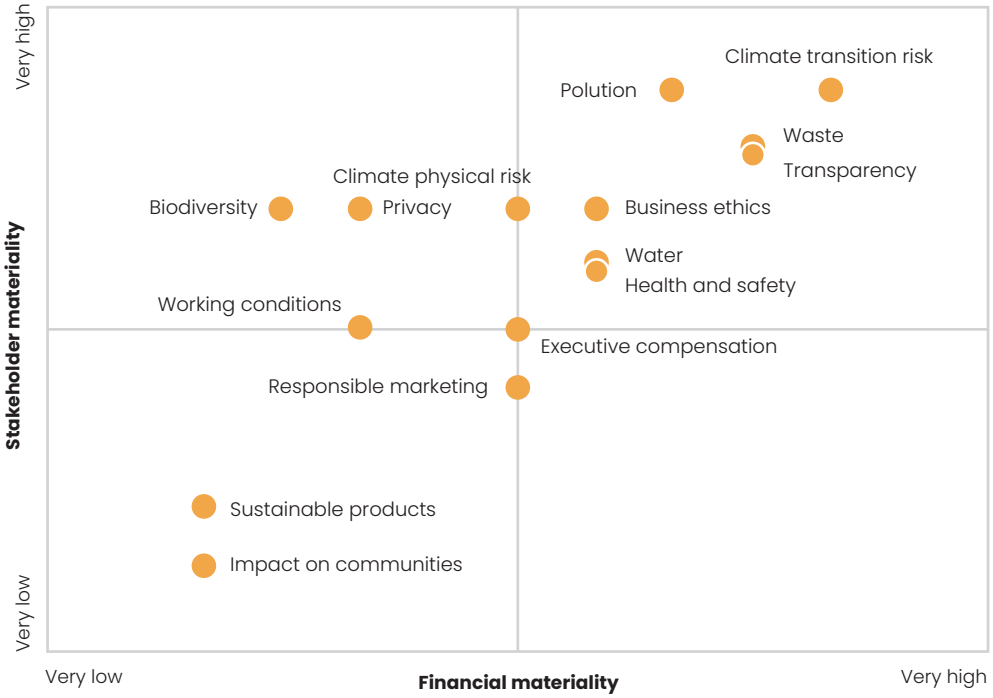
2 What is the role of privacy in the ESG landscape?

Rating agencies are now looking at privacy

ESG reports and ratings are growing in importance as investors and stakeholders increasingly rely on them to better understand the non-financial performance of organisations. Sustainalytics is one of a few rating agencies with a dedicated data privacy and security section. However, the focus is on cybersecurity with references to ISO and SOC2 certifications. This limits the effectiveness for businesses with good data privacy and data governance programmes to demonstrate the links between ESG and privacy.

Standard and Poor's (S&P) also have a detailed focus on data privacy for deriving credit and ESG scores, both of which can have a significant impact on an organisation. Low credit scores make it harder for companies to borrow money. A poor data governance programme can therefore have a negative impact on a business using S&P's scoring system. S&P have developed a materiality maturity model that features privacy amongst other sustainability factors.

Example of an ESG Materiality Map for the ABC Sector



Source: S&P Global Ratings ESG Materiality Map

Note: The ESG factors shown on the map are some examples and not necessarily the actual ones used by S&P Global Ratings or S&P Global Sustainable. The sector shown is meant to be hypothetical. Source: S&P Global Ratings.

Standards on ESG disclosures are evolving

There are some existing privacy and security global standards from the Global Sustainability Standards Board (GSSB) based on the Global Reporting Initiative (GRI), detailed in the Annexes, GRI 418, Customer Privacy 2016[5], which has been effective since July 2018. However, there is currently no baseline or clarity as to what organisations should be disclosing about their data governance practices, for effective ESG scoring.

Organisations are now starting to recognise the importance of the work done on data governance to their ESG credentials. Recently, and now more frequently, companies are choosing to add additional materiality measures to their annual ESG reports in order to complement GRI standards.

Examples are numerous and varied and include dedicated privacy web pages, online privacy training, privacy dashboards and self-service portals, Q&A with senior leaders, blogs about privacy by design and data security, as well as privacy awareness campaigns such as Data Privacy Day. This demonstrates the importance of privacy and data governance to many organisations. The fact is, there has been an increase in customers' expectations when it comes to the protection of their personal data. This is driving change.

Despite the shift in the privacy landscape there is a distinct lack of organisational-level privacy certifications, ESG related or otherwise.

This makes it difficult for organisations to show the maturity level of their privacy programmes. Those companies that do fall short, likely due to data breaches, have seen trust evaporate and damage to their brand.

There is an opportunity here. Good privacy programmes and their disclosure promotes data hygiene, which protects the data of customers, employees and vendors. This determines the levels of trust consumers have in the market and organisations, also positively influencing ESG ratings.

Privacy principles developing faster than ESG

There is little consistency when it comes to scoring privacy at rating agencies. The value of the ratings and reports are also diminished due to the criteria used in assessments – namely a greater weighting on environmental issues and less of a focus on privacy related matters.

Despite significant regulatory developments in privacy and data protection globally, there has not been an equivalent shift in ESG reporting and ratings to match the massive uptick in

5. GRI 418: Customer Privacy, GRI Sustainability Reporting Standards, 2016

investment, focus and attitude towards data privacy since 2018. Many new privacy regulations have been implemented or updated since then improving privacy principles globally.

ESG reporting space is starting to mature

In response to a lack of consistency in reporting, organisations have looked for standards to align themselves to. The Global Reporting Standard (GRI) is now popular, its disclosures focus on the number of identified data leaks, losses and thefts of customer data.

The European Union is working on mandatory ESG disclosures as part of the Corporate Sustainability Reporting (CSRD). However, data protection is not highlighted as a significant concern within this initiative. The financial sector is now moving towards mandatory disclosures. Regulatory bodies are also actively defining guidelines. Again, the one consistent theme is the lack of privacy related requirements.

The creation of the International Sustainability Standards Board 'ISSB' of the International Financial Reporting Standards is the most significant recent development. This is a big leap towards a more unified ESG reporting landscape. There is hope that ISSB standards will become the global baseline effective from 2024. Each country will have to decide whether to make these mandatory. Again, privacy metrics are excluded from this reporting process.

Aligning privacy principles with ESG is vital

Global privacy regulations align on several key principles, namely lawfulness, transparency, fairness, accuracy, purpose limitation, storage limitation and security and offer similar rights that apply to individuals whose data is being processed.

Broadening the privacy aspect of ESG ratings to a wider set of privacy principles is crucial. How well an organisation is adhering to these principles will provide a holistic and more accurate assessment of an organisation's privacy maturity. This will also help to articulate what privacy means in the context of ESG.

Right now, determining the ESG risks posed by data privacy is still in its infancy particularly when it comes to reporting. A significant challenge is metrics, in the next chapter this topic is discussed further.

3 How can organisations elevate and calibrate privacy-ESG metrics?

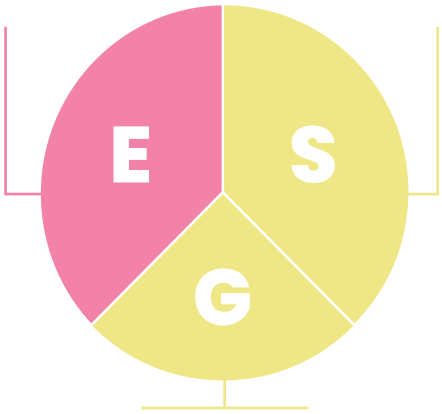
What does good look like when it comes to metrics?

Core activities needed to comply with data regulations and ensure an efficient privacy and data protection program can be mapped against 'E', 'S' and 'G' components and their potential benefits. Compliance with these core activities should all be considered by businesses and rating agencies when assessing ESG credentials. The aim of identifying the core activities that have an ESG impact is to drive consistency in assessing ESG credentials, irrespective of business sector, create metrics, assess the significance and demonstrate maturity. This will allow businesses to measure their privacy impact and identify areas for improvement.

Note that some of these metrics below, could be adopted internally to gauge their maturity level within organisations. What is then externally disclosed and how this can be compared to peer organisations within the related industry requires further work to ensure it provides a fair and protected representation across companies.

Customer Rights Requests: The centralisation of data, process simplification and automation drives greater control for businesses when complying with requests.

This reduces volumes of data stored and processed (both electronic and paper) form, reduces complexity and scale of processing.



This helps link customers to their data, driving greater transparency, trust and enhances brand value. Provides customers with the ability to determine the impact of processing operations.

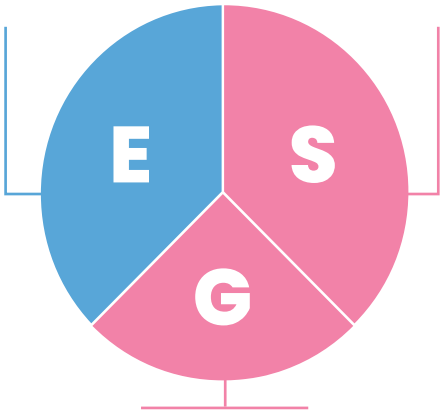
This simplifies governance and facilitates better handling of customer requests.

Suggested maturity/indicators: *Percentage of requests handled in a time frame, and delivered electronically, average time taken to respond, number of unresolved complaints.*

Key: High Importance | Medium Importance | Low Importance

Transparency: Greater use of on-line and just in time notices delivering a layered approach, facilitates greater clarity around how personal data is used yet allows access to more relevant, comprehensive and detailed explanations.

This reduces customer enquiries and 'back and forth' communications reducing data processed and paper-based notices.



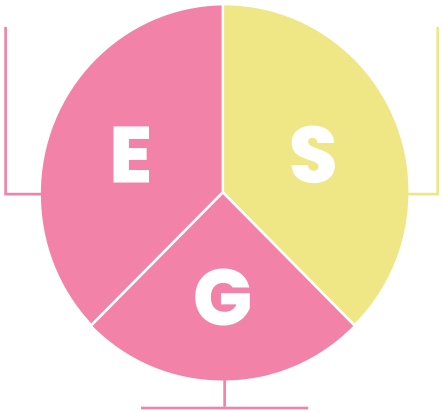
This provides greater clarity to customers and society on how data is processed and used. Drives ethical use cases. Promotes trust and allows customers to raise concerns over the use of their data.

Online notices allow companies to assess number of times they are viewed helping firms monitor customer interest and awareness and measure privacy notice effectiveness.

Suggested maturity/indicators: *Number of complaints or enquiries, number of times the full privacy notice is accessed.*

Privacy by Design & Default: By implementing upfront data assessment as part of product/process design or change allows companies to safeguard privacy and data protection principles and uphold rights.

This facilitates data minimisation reducing the volumes of data collected and processed.



By increasing the functionality of user profile settings, this allows greater control over customer data. This promotes trust among users and places them in charge of their data.

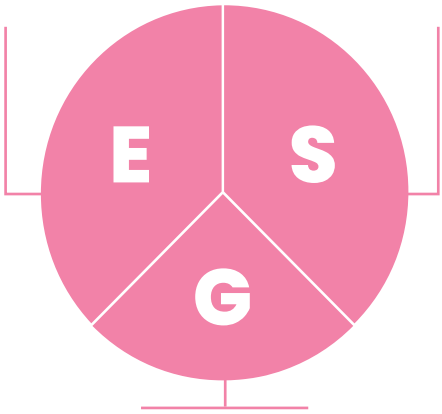
This strengthens a company's approach to risk and control management, ensuring controls are appropriately design and implemented. Encourages the use of Privacy Enhancing Technologies (PETs)

Suggested maturity/indicators: *Percentage of projects with privacy assessments during development; number of privacy features integrated; instances of non-compliance; % of change programmes using live data in test; number of training programmes for privacy.*

Key: High Importance | Medium Importance | Low Importance

Data Breach Prevention (Process and breach handling): Enhanced data mapping and development of data incident response strategies and plans. Approach supported through improved automation.

Direct environmental impact may be limited, increased focus on breach prevention drives greater consideration as to how obsolete hardware is disposed of.



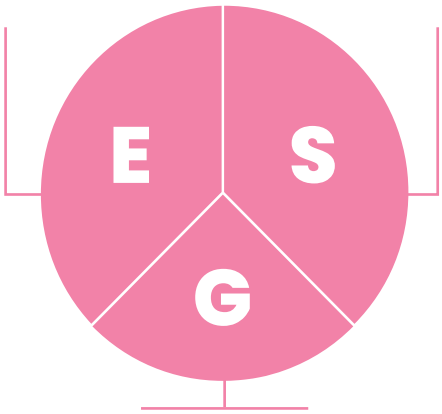
Drives greater trust that companies have strategies in place and upholds rights to protect data and be transparent should a process materialise. Monitoring root causes of 'small' breaches and addressing control weaknesses improves prevention. Minimise negative impact of processing data.

Well documented governance arrangements that allow the ability to assess and contain at pace potentially reducing scale and materiality of harm.

Suggested maturity/indicators: *Average time taken to identify and contain data breaches, cost per data breach incident, including legal, financial, and reputational impact; breach recurrence rate over a specific period, Number of reportable breaches.*

Data Discovery and Mapping: Automation of discovery, mapping and improved processes to manage and document what a business holds and where third parties process a company's data.

Discovery and of redundant, over-retained and duplicate data and records leads to deletion or destruction of that data, reducing paper and electronic storage.



Customers can trust that they know where and why their data is processed and that their rights can be respected and upheld.

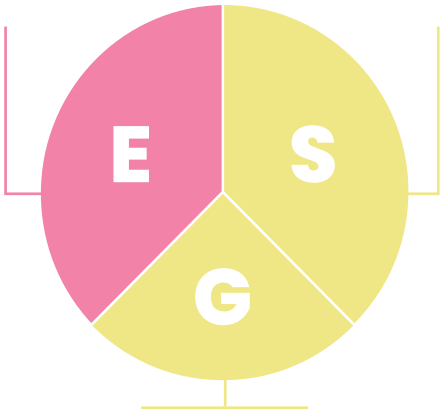
Knowing where data is stored and processed is fundamental to effective privacy management.

Suggested maturity/indicators: *Percentage of sensitive data discovered by automated tools; False positive rate of automated data discovery tools; Time taken to detect and classify types of data including sensitive data; Percentage of suppliers with data discovery and disposal tooling.*

Key: High Importance | Medium Importance | Low Importance

Retention and Disposal Processes: Policies and procedures that ensure data is only processed for as long as it's necessary, simplification of IT estate and automation of disposal processed (including 3rd parties)

This reduces the volumes of personal data processed and the amount of hardware used.



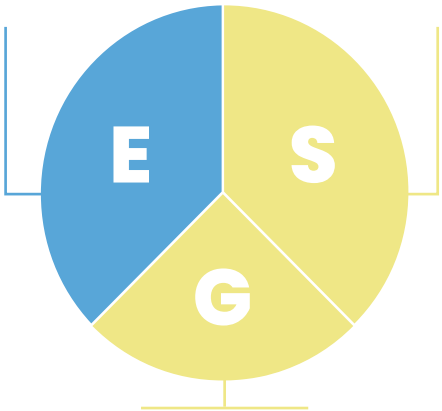
This upholds the right of erasure and increases trust that data is only used for the purpose it was intended.

Improves ability to measure and report the volumes of data disposed of.

Suggested maturity/indicators: *Percentage of data retention compliance within defined timeframe; Average time taken to fulfil data deletion requests; accuracy rate of tracking data retention periods for different data types; % of systems with disposal capability; % of systems containing over retained personal data; number of physical records containing over retained personal data.*

Consent Management: Potential to automate and simplify the processes, improving customer experience, building trust, and helping drive compliance with GDPR/PECR.

This reduces the different forms and processes in place and the amount of paper used.



This increases the level of control customers have over how their data is processed, increasing trust. Reduces the levels of nuisance calls and unsolicited mailing. Ensures customers understand that when customers contact them it is relevant to the services/products provided.

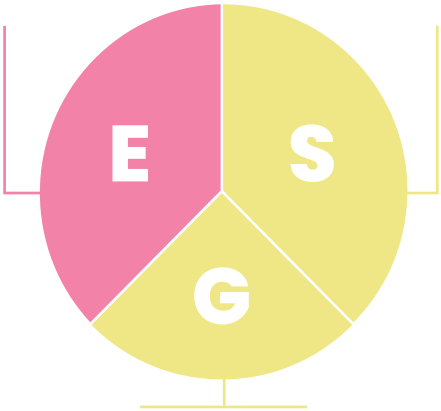
Automation of consents strengthens the ability to manage, including right of withdrawal and effective audit trails.

Suggested maturity/indicators: *Having the capability to allow for consent and manage it; percentage of users providing explicit consent; opt-in and opt-out rate for consent options; frequency of consent reviews and updates; % of consents managed electronically.*

Key: High Importance | Medium Importance | Low Importance

Culture: Ensure staff are aware of their privacy responsibilities and supported through qualified colleagues, privacy policies and procedures.

This facilitates data minimisation, effective retention and disposal and upholding rights – reducing the volumes of personal data processed and their environmental.



A privacy culture facilitates privacy by design and through default, promoting transparency and driving personal accountability. This supports a diverse and inclusive workforce that aligns to its customer base.

Clear roles and responsibilities and privacy structure in companies.
Privacy agenda driven from the top.

Suggested maturity/indicators: *Participation rate in privacy training programs; average score on post-training assessments; number of privacy-related inquiries from employees over a specified period; Percentage of qualified privacy colleagues; Number of privacy certifications.*

Key: High Importance | Medium Importance | Low Importance

How can privacy principles impact ESG scores?

By adhering to good data privacy, data ethics, cybersecurity and data governance practices an organisation can set their risk 'appetite' and measure performance against this appetite - demonstrating tone from the top that will in turn help proactively manage their data risks, protect data and enable it to be used safely within the organisation. This also resonates with ESG factors since good privacy principles result in increased customer and employee trust, as well as a lower carbon footprint.

Research shows that the following privacy principles, count positively towards ESG scores:

Data minimisation: Only data needed for legitimate data processing should be collected and maintained, reducing unnecessary data. More data means a greater carbon footprint and more social, as well as governance and security issues.

Data retention: Data that is no longer necessary should be deleted, resulting in data reduction on servers and on the cloud. This can also lead to the decommissioning of on-premises legacy platforms, all of which reduces the carbon footprint.

Data subject rights: Data subjects have rights such as to access or delete their data. Handling such requests in an automated way and providing an online portal for customers reduces the amount of paper and postage. It also makes the process and manpower more efficient internally.

Privacy by design: Privacy requirements should be incorporated at the outset of any new data processing. By doing so, organisations reduce the potential misuse or loss of personal data, which is good for legal compliance and customer trust in an organisation.

Transparency: Data subjects should receive clear information on how their personal data is used, enabling customers to decide if they want to engage with an organisation, raise their concerns and ultimately, promote customer trust.

Training & awareness: Utilising interactive training measures together with employee engagement activities, such as Privacy Day and newsletters, fosters a culture of organisational privacy and good data governance.

Data hosting: Reviewing data hosting and storage options helps with carbon footprint. For example, by relying on multi-tenant data centres for digital data storage, offering them the chance to minimise energy consumption by utilising shared facilities for data storage in a secure way.

Use of technology: New technology utilising available data can help businesses to assess their environmental score. For example, organisations can employ sustainability applications to evaluate and quantify the carbon footprint generated by IT infrastructure. This enables organisations to make decisions on hardware procurement. Organisations can actively participate in data retention and deletion policies by accessing real-time sustainability data relating to IT hardware.

Supply chain: Organisations should also look at their supply chain for further gains, for instance, providers of asset lifecycle management services (AML), help customers to safely dispose of their data and reutilise valuable minerals.

These are still early days for the quantification and qualification of privacy-ESG metrics. Certainly, global standards can help better define how to calibrate and align privacy with ESG. This is covered in more detail in the next chapter.

4 When will ESG and privacy be reported together?

There's common ground for privacy-ESG standards

The global privacy ESG standard, GRI 418: Customer Privacy 2016[5] is not sufficient enough to determine the effectiveness of the data privacy function across an organisation. Typically, consumer facing organisations such as those in retail or consumer banking are much more likely to receive a greater number of internal and external data subject requests than those focused on industry or B2B.

Quantitative measures therefore could be increased to cover additional key data privacy performance indicators (KPIs). However, these do not provide the full picture, particularly in the effectiveness of privacy governance and day-to-day practices to protect data within a business, this is why additional qualitative measures are also recommended.

A data privacy maturity assessment, ISO 27701 certification (Security Techniques)[6] or similar regular review across a framework of measures provides a level of maturity for each privacy activity which has been identified as providing value in the ESG arena.

Based on the AICPA, GAPP Privacy Maturity model, there are five levels of maturity (ad-hoc, repeatable, defined, managed, optimised). These could be used to score different privacy activities such as the DPIA process, handling of website cookies and privacy policies.

This white paper is not stipulating one specific privacy maturity assessment at this time, but if an organisation regularly conducts privacy assessments, they can use this to demonstrate to ESG rating providers their level of privacy maturity. This can provide a qualitative view, supplementing quantitative measures laid out in the GRI standard. Such maturity assessment models shows that an organisation is taking action on material risks to customers and has a defined approach to manage such risks.

In addition to regulatory based privacy maturity assessments, there is also interesting work being conducted by the Maastricht University on 'Data Protection as a Corporate Social Responsibility Controls' (DPCSR Framework).[7] The aim is to focus on areas of data protection that can benefit society, with five principles and 25 rules. The objective is for organisations to sign up to this certification. By having such a framework this could be another measure that will contribute to an organisation's data privacy ESG score.

5. GRI 418: Customer Privacy, GRI Sustainability Reporting Standards, 2016
6. ISO/IEC 27701: Security techniques, focused on privacy information management, 2019
7. Data Protection as a Corporate Social Responsibility, European Centre on Privacy & Cybersecurity, March 2022

Rating agencies role is crucial in privacy-ESG alignment

One way to create a degree of consistency is through ESG rating agencies such as S&P and Moody's. If these agencies use a comprehensive data privacy assessment they could deploy this across all companies they assess. This would be the first step in bringing consistency and enable companies to be benchmarked. It could also help agencies demonstrate the value that data privacy contributes to ESG and justify the investments needed.

In its 2023 questionnaire, the S&P rating agency included details on data privacy, focusing on publicly available information and evidence. The questionnaire allows companies to provide for more qualitative description of their privacy programmes. This is detailed in the Annexes.

The philosophy of the newly adopted European Sustainability Reporting Standards (ESRS) as published by the European Commission in July 2023, is different. Under ESRS S4 "Social"[9], the organisations subject to mandatory corporate sustainability disclosure requirements have to disclose information relating to engagement with consumer and end-users. This is detailed in the Annexes.

Transparency and data privacy maturity are challenges

ESG rating agencies need a good source of information on data privacy maturity. Some agencies go into organisations with questionnaires, which is a positive step, while others struggle to get information they need from reviewing company ESG reports, secondary internet research or content from company websites.

Greater transparency between organisations and ESG rating providers would improve the scoring of organisations. It's therefore important to ensure a high level of internal coordination and evidence tracking. This can be shared with rating providers, corporate reports and websites, boards, shareholders and the media.

The environment in which privacy and ESG standards operates has some way to go before it comprehensively covers both functions, in the meantime what can organisations do now to proactively engage in practices that promote privacy and ESG? The next chapter discusses this further.

8. Corporate Sustainability Assessment 2023, S & P Global
9. European Sustainability Reporting Standards, ESRS S4 Consumers and end-users, Draft November 2022

5 How can industry be more proactive on privacy and ESG?

A set of new guidelines will help

It's time for a series of actions that cut across industries:

- Privacy and data leaders should have a voice at the executive table when ESG is being discussed and closer links with their ESG counterparts and sustainability teams.
- ESG ratings must embody a wider set of privacy principles. How well an organisation adopts these principles determines privacy and data governance maturity, this could then affect ESG scores.
- Organisations need a new global privacy ESG standard, a comprehensive data privacy assessment used consistently across all rating agencies to take data considerations into account when giving ESG scores.
- A global privacy ESG standard would demonstrate the value that privacy contributes to ESG, such a tool could create a virtuous circle of investment.
- Privacy assessments should start to calibrate ESG factors, pushing further automation, use of privacy enhancing technologies and introducing ESG considerations for data protection impact assessments (DPIA), legitimate interest assessments and data mapping.
- Establish a broad consensus of quantitative and qualitative measures that organisations could use to disclose securely their data privacy maturity level.
- Engage with ESG rating providers active in this field and others who are looking at privacy and data governance in more detail to see if a level of consistency is possible.
- Look to quantify and qualify how privacy assessments could help with the ESG scores of organisations.

Privacy could be more ESG focused

Seeing privacy through an ESG lens can help, examples include:

1. Stepping up privacy automation

Moving to automated tools not only removes all the paper it also saves time and improves quality and collaboration. Having your core privacy processes on an automated tool with workflow management tools improves maintenance and hence the sustainability and maturity of privacy activities.

2. Use privacy enhancing technologies (PETs)

By using PETs, organisations are able to de-identify data so it's no longer personal and can then be used and shared or pseudonymised so during a clinical trial a person with a health condition can be contacted again if a treatment is offered to them. Even using synthetic data for testing and AI datasets can de-risk harm to individuals.

3. Add ESG questions into DPIA or ROPA assessments

Add questions to Data Protection Impact Assessments (DPIA) and Record of Processing Activities (ROPA) that go beyond the legal requirements of data protection e.g., how sustainable are your third-party vendors? Questions relating to corporate social responsibility such as the Maastricht University DPCSR could be included.

How to integrate privacy with ESG factors

Organisations that go beyond compliance and integrate privacy into their ESG initiatives could stand out. Adopting some of these practices will help:

1. Engage regularly

Elevate privacy and data governance thought leadership. Regularly bring up privacy risks and recommend mitigations, deliver privacy update sessions to the board using presentations, newsletters and workshops. Ensure the board remains informed about evolving privacy regulations, imminent risks, best practices, and the organisation's current compliance landscape. Highlight case studies and real-world implications. Showcase where privacy and data protection compliance can act as a differentiator.

2. Collaborate with ESG teams

Identify synergies between privacy and ESG goals, streamline resources and foster shared ownership of goals. For instance, assessing the impact of data storage solutions on an organisation's sustainability targets or pushing joint campaigns highlighting ethical data practices, or the social dimension of ESG through training and upskilling the workforce.

3. Integrate privacy with ESG strategies

Demonstrate how privacy and data protection are related to ESG objectives. Suggest joint budgeting for common projects. For example, investing in data disposal projects improves privacy compliance, but also reduces cloud computing needs, cuts the carbon footprint and energy costs.

4. Demonstrate ROI

Outline returns from privacy initiatives and link these returns to ESG goals. For instance, investing in better data management and security practices can lead to fewer data breaches, translating to financial savings from potential fines. Furthermore, optimised policies and data processing activities can reduce unnecessary data storage and a lower carbon footprint.

5. Benchmark progress

Regularly assess the organisation's practices against industry standards, feedback from rating agencies and competitors. Use insights to identify areas for improvement, potential risks, and opportunities for innovation. Provide the board with data-driven insights so they can be strategic about privacy and ESG.

6. Align activity with ESG reporting

Privacy and ESG should go hand in glove. Ensure personnel are informed in advance of what input is expected on privacy, such as responses to questions from rating agencies, as well as look for opportunities to make privacy more prominent by disclosing information about achievements, long term goals, potential risks and strategies to address issues. Look to reinforce trust from external stakeholders in the organisation's privacy practices.

Conclusion

These are still early days for privacy and ESG. There is no doubt though that privacy principles and data regulation will be one of the key, next pillars in the ESG revolution. As we've seen in this white paper, privacy has a pivotal role to play in the ESG landscape. However, further calibration will be crucial in order to quantify and qualify how adhering to good privacy principles can raise ESG ratings.

There will come a time when privacy and ESG are reported together, although a lot more groundwork needs to be done. It will take an ecosystem approach whereby global standards are agreed upon, where legislation and regulation coalesce around privacy and ESG metrics, spearheaded by a proactive approach from industry on this topic.

A lot more work needs to be done. It is hoped that this white paper starts to lay the foundation. Both privacy and ESG can be powerful allies in building a more ESG friendly future, which has privacy principles at its core.

6 Appendices

References

1. Data Protection and Privacy Legislation Worldwide, United Nations Conference on Trade and Development (UNCTAD)
2. Making AI Less "Thirsty": Uncovering and Addressing the Secret Water Footprint of AI Models, Pengfei Li, Jianyi Yang, Shaolei Ren, UC Riverside (Cornell University, Arvix)
3. Gartner Unveils Top Predictions for IT Organizations and Users, IT Symposium October 18, 2022
4. Large, creative AI models will transform lives and labour, The Economist, April 2023
5. GRI 418: Customer Privacy, GRI Sustainability Reporting Standards, 2016
6. ISO/IEC 27701: Security techniques, focused on privacy information management, 2019
7. Data Protection as a Corporate Social Responsibility, European Centre on Privacy & Cybersecurity, March 2022
8. Corporate Sustainability Assessment 2023, S & P Global
9. European Sustainability Reporting Standards, ESRS S4 Consumers and end-users, Draft November 2022

Annexes

Global Reporting Initiative Standards 418 & 410

GRI 418: Customer Privacy 2016

Disclosure 418-1:

Total number of substantiated complaints received concerning breaches of customer privacy, categorised by:

i. complaints received from outside parties and substantiated by the organisation;

ii. complaints from regulatory bodies.

b. Total number of identified leaks, thefts, or losses of customer data.

c. If the organisation has not identified any substantiated complaints, a brief statement of this fact is sufficient.

GRI: 410 Security Practices 2016

Disclosure 410-1:

1. Security personnel trained in human rights policies or procedures

2. Percentage of security personnel who have received formal training in the organization's human rights policies or specific procedures and their application to security.

3. Whether training requirements also apply to third-party organizations providing security personnel

S&P, 2023 questionnaire

3.8 Privacy Protection

Networked data and globalised corporate activities require careful handling. Insufficient database and network protection, unclear management of personal information and vague database access rules could expose companies to large risks in case of personal data leakage and misuse, or unauthorized access. For companies to avoid legal costs, reputational risk, and exclusion from certain activities, a company-wide privacy policy is paramount. Our questions focus on the coverage of the company's privacy policy and the mechanism in place to ensure the policy's effective implementation.

3.8.1 Privacy Policy: Systems/ Procedures

What mechanisms are in place to ensure effective implementation of your company's privacy policy?

3.8.2 Customer Privacy Information

This question requires publicly available information.
This section includes a mandatory challenging question on the following:

We monitor the percentage of users whose customer data is used for secondary purposes. Please indicate the percentage of customers whose data is used for secondary purposes and provide publicly available evidence.

ESRS S4 Consumers and end-users

Policies related to consumer and end-users (S4-1) *- it can be assumed that the customer facing privacy transparency obligations definitely fall into this category and privacy policies will be an important element of this disclosure requirement; This can be accompanied by a more programmatic disclosure related to the maturity of transparency requirements and privacy settings;*

Processes engaging with consumers and end-users (S4-2) *– the individual rights requests process to address individual rights also appear to be in scope for this disclosure requirement as they allow users to engage with the organisation processing their personal data; Engaging customers for user testing of privacy features may also find its place in this disclosure requirement.*

Processes to remediate negative impacts and channels for consumers and end-users to raise concerns (S4-4) *– within this disclosure requirement, one can see the importance of the incident management process, channels of communication with the Data Protection Officers/privacy offices, processes for exercising individual rights as a way for consumer and end-users to raise their concerns on the processing of their personal data.*

Taking action on material impact to consumer and end-users and approaches to managing materials risk and measuring effective of such actions (S4-4) *– if privacy is identified as a material risk under the double materiality assessment, under this disclosure requirement, the importance of a privacy programme and measing its efficiency through various KPIs can be disclosed. Companies may also want to disclose the scope of user settings and controls that they provide to their customers.*