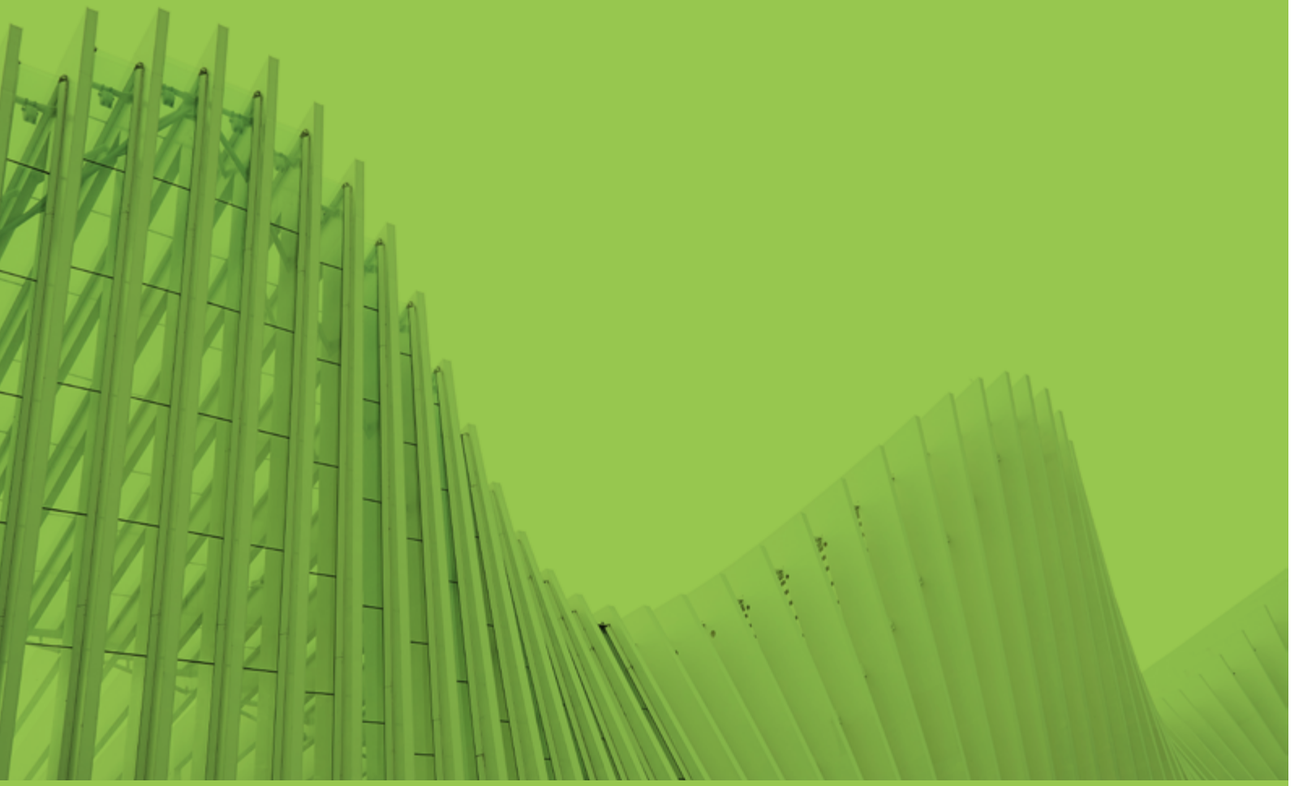
GLOBAL PRIVACY CULTURE SURVEY

ANNUAL REPORT

2021



Contents

Executive Summary

To understand and improve an organisation's approach towards data protection and privacy compliance starts by understanding cultural attitudes and behaviours. This is particularly important right now when the boundary between privacy at 'work' and 'home' is even more blurred.

The global cost of **GDPR compliance** was **$7.8billion** for USA's top 500 organisations and **$1.1billion** for the UK FTSE 100 organisations.

— IAPP and EYR

Privacy Culture Limited has over 75 years collective experience in embedding data protection, privacy, governance and security into large and often disparate global organisations and have compiled this research in conjunction with **Queen Mary University of London**, **Dentons** law firm, and **Capgemini**.

We recorded the behaviour, attitude, perceived control, knowledge, and culture of over **3,000** anonymised employee respondents from **10 global organisations** spread across six industry sectors, geographically represented across **52 countries**, and obtained feedback from **16 functions** including Marketing, Human Resources, Customer Services and Technology.

The top three performing themes from the survey across all industries were **Data Breach and Incident Management**, **Governance and Accountability,** and **Compliance and Monitoring**. This is heartening for DPOs and CISOs alike as our follow-on workshops indicate that some of the foundational elements of privacy and security i.e. how to recognise and report a potential data incident, are landing with 97% of respondents feeling confident that they can recognise the consequences of not reporting a data incident.

However, digging deeper into the survey results and through the workshop conversations, we found that **data sharing** and **deletion** still causes confusion, particularly when dealing with third parties, in addition to which it was also apparent that the ability to recognise and report an **individual data rights request** is not always clear.

The five lowest performing themes across all organisations were **Risk Management**, **Records of Processing**, **Retention and Deletion**, **Transparency** and **Policies, Training, Awareness and Culture**. It's notable that these themes include more technical aspects of data protection, privacy, security, and governance, and knowledge and behaviour will be heavily dependent on the maturity of an organisation's data protection and privacy programme, as well as whether concepts such as the Data Protection Impact Assessment feature in general on-boarding and annual compliance training.

Every organisation wants to improve compliance and reduce regulatory risk whilst maximising the use of personal data and improving employee relations. The world's first global employee privacy culture survey can help achieve this through prioritised areas of improvement and enhancing attitudes to privacy across the workforce.

We hope you enjoy the first Global Privacy Culture Survey Report.

Foreword

This report is a result of collaboration between four leading institutions. It is a unique, authoritative and indispensable snapshot of employee's culture of data protection, privacy, security and governance, captured in a time of global pandemic. It makes for compelling reading for organisations, DPOs, CPOs, CISOs, and CDOs alike, and goes a long way towards illustrating how and why culture is such a significant factor in influencing the hearts and minds of employees. Continuing this important work, the survey will monitor, benchmark and track these trends for the next 10 years.

Here, our partners give us their views on why this is such an important undertaking for them, their clients and students, and for the industry as a whole.

Contributors

Victoria Guilloit
Partner
Privacy Culture

Steve Wright
Partner
Privacy Culture

Alistair Cole
Partner
Privacy Culture

Ian Walden
Director, Centre for Commercial Law Studies, **Queen Mary University of London**

Graham Hunt
Director, Risk, Regulation and Compliance, **Capgemini**

Simon Elliott
Partner, Privacy & Cybersecurity, **Dentons**

Antonis Patrikios
Partner, Privacy & Cybersecurity, **Dentons**

Nick Graham
Partner, Privacy & Cybersecurity, **Dentons**

> By identifying how law and regulations are understood within organisations and influence behaviours and attitudes at an individual level, this survey enables us to critically assess the relevance and effectiveness of such rule-making."–*Ian Walden*

> This report takes a fresh look at privacy compliance by exploring how privacy is working from an individual perspective within organisations. Don't lose sight of these people insights–they are key to assessing the success of your frameworks and controls"–*Nick Graham*

PrivacyCulture

The most important part of any organisation is its people and here at Privacy Culture our team members are all passionate advocates for privacy rights, law, security and bringing about culture change in organisations.

Our lawyers, privacy engineers and consultants love to be in the thick of it when it comes to problem solving; not only are they tenacious, dedicated and professional, they all want to make a difference, make the change stick and embed that culture of privacy.

We're not just well-qualified to provide advice and support; we're creative and innovative and bring that difference in our approach.

Capgemini

David Brin, the scientist and author once said: "When it comes to privacy and accountability, people always demand the former for themselves and the latter for everyone else." This is also true of organisations and governments.

Capgemini is an international technology firm that consults and delivers for its clients – helping protect, govern and gain insights with data. Our experience is that implementing data privacy measures is one thing but making that sustainable and instilling a sense of accountability can be far harder to achieve.

That's why we at Capgemini are pleased to support this world-first report on the attitudes and culture of privacy within organisations.

大成 DENTONS

Dentons is the largest law firm in the world. It has offices in 204 locations in 81 countries and a dedicated Global Privacy and Cybersecurity Group that advises large corporate groups and organisations on data protection and cyber incident risk across all geographies. Our clients include big data and tech companies, retailers, adtech, household names and other large organisations and their DPOs.

Dentons is delighted to participate in this Privacy Culture survey and is excited to observe global notions of employee privacy practices and sentiments that will provide deep behavioural insights. We hope this survey will encourage others to participate, to share global trends experience and ask how this survey can impact their organisations.

Queen Mary University of London
Centre for Commercial Law Studies

The Centre for Commercial Law Studies at Queen Mary University of London is a unique institution that focusses exclusively on the study of commercial law at a post-graduate level.

CCLS has been researching, writing and teaching about privacy and data protection issues for over 30 of its 40 years of existence. We are pleased to partner with Privacy Culture on this survey, offering our students an opportunity to gain valuable experience, as well as contributing to impactful research in this increasingly important area of commercial practice.

The focus of this survey and the breadth of participants will offer important new insights to those that practice in, or are impacted by, this increasingly regulated space.

What do we mean by ‘a culture of privacy’?

It will come as no surprise that “what does a privacy culture look like?” is a question that is frequently asked of us here at Privacy Culture.

> Privacy tools, eLearning and compliance, in isolation, will not change the culture or improve the collective knowledge, attitude, or behaviour of an organisation.”

Tianya Li wrote a paper on organisational culture and employee behaviour for the Lahti University of Applied Sciences 20151, in that she defined culture as “the way we do things around here”. Culture affects employee behaviour; the research question cannot be answered based on numerical data alone. In other words, privacy tools, eLearning and compliance in isolation will not change the culture or improve the collective knowledge, attitude, or behaviour of an organisation.

Given that the GDPR only came into force in 2018, it has not taken long to realise that demonstrating compliance through annual training alone is not enough to give DPOs comfort that, when the time comes, employees are able to recognise and react to privacy risks or data breaches.

A common misconception is that a culture of privacy is the conclusion of an awareness, education and training programme that goes beyond the basics and gets to the heart of what individuals need to do to manage personal data appropriately in the context of their role. Although this is a key requirement of ensuring employees have the appropriate knowledge, it does not necessarily mean they believe that they, or their organisation, have an ethical duty to do the right thing with personal data, or that they feel personally empowered to make appropriate decisions surrounding the data.

Our view of ‘privacy culture’ is that, first and foremost, the organisation is transparent about what they are doing with the personal data of customers, suppliers, and employees; and they will only do this with confidence when they are sure that their personal data infrastructure is in good shape. By this, we mean that they really know where their personal data is, where it comes from, what it’s being used for, whether they have the correct and appropriate legal basis for processing it, and that it is protected in transit and at rest. If, for any reason, something does go wrong, the impact will be kept to a minimum because the workforce knows what to do–and will act quickly, and with confidence.

This is no small ask, particularly where businesses operate across different geographies with varying local cultures; many of which may be resistant to change. The requirement to gather and balance employee views on how well they believe their organisation understands and applies data protection and privacy with the policies, processes, procedures, and programmes in place emerged through Privacy Culture’s GDPR and Privacy Maturity Horizon™ framework. This framework helps organisations to understand how much work they need to do to build a defensible position and demonstrate compliance with existing and emerging data protection and privacy laws globally.

The annual cost of GDPR non-compliance in 2020:

€182m

–IT Governance

The Global Privacy Culture Survey

An overview of the methodologies, standards and processes behind our ground-breaking employee privacy culture survey.

Our 50-question survey organised around 12 key themes of data protection and privacy, from Governance and Accountability through to Compliance and Monitoring (see Appendix for full listing) is designed to elicit employee knowledge, attitude and behaviour. It provides an indication of how much control employees believe they have over the associated processes and procedures, as well as how much influence the organisation has over their effectiveness across different locations, functions, or operating companies.

Employees are asked to decide, based on a seven-point Likert scale, to what extent they agree with a statement; there are no non-applicable answers. Participants are asked to respond according to what they do now, as well as what they would do if faced with a new situation; for example, to what extent would they engage with the Data Protection Impact Assessment (DPIA) process when doing something new with personal data. Responses to the survey are anonymous to all parties, however pre-screening questions include basic information about role, function, and location. This enables us to inform participating organisations where they may need to target remedial action, such as awareness campaigns, education, training, or data governance, policy, process and data system improvements. It also enables us to make cross-organisational comparisons across all participants equally.

The survey is supplemented with workshops where employees are invited to share their views on the subjects of data protection, privacy and governance in their organisation. In our experience, allowing employees the freedom to have their say about topics which have prevented them from doing the right thing at the time–especially in times of economic strain, provides a deeper insight and additional context where the survey has a wide regional or functional reach.

It’s important to note that, although the survey process is comprehensive, it cannot be taken as an assurance of compliance or otherwise. What it will do is give an indication of what employees are doing right now and why, which is invaluable when determining where to prioritise data protection and privacy activities.

Our Rating System

How results are measured

Rating	Score	Description
Satisfactory	6.50 or above	Your organisation frequently shows the desired behaviours and attitudes required to embed a good culture of privacy and data compliance. **A periodic and systematic review of the survey outcomes should be actioned to continue maturing your privacy culture.**
Inconsistent	6.00 to 6.49	Your organisation shows some of the desired behaviours and attitudes required to embed a culture of privacy and data compliance. There may be specific locations or functions that require attention to further enhance the messaging, governance and structure of your privacy operations. **A review of these areas is necessary to ensure consistency across your organisation.**
Unsatisfactory	5.00 to 5.99	Your organisation needs to review the gaps identified and **take the necessary actions within six months to a year.** Examples might include insufficient training for specific audiences, low awareness among staff and incoherent privacy action on the specific issue.
Poor	4.00 to 4.99	Your organisation needs to **resolve gaps identified and take the necessary actions within the next 3-6 months**. Examples might include inadequate training, tools not rolled out or incoherent policies and practices surrounding data and privacy practices.
Failing	0 to 3.99	Your organisation needs to **immediately address and resolve the gaps identified**. Examples might include inadequate privacy resources, little or no training, poor tools or lack of general data awareness and data ownership of the specific issue.

2021 Results: Overview

Every organisation wants to improve compliance and reduce regulatory risk; whilst responsibly utilising personal data and improving employee relations. This global research and the report recommendations can help ensure prioritised focus on areas where employees do not feel empowered, educated, or confident in using and accessing personal data from around the globe.

> This Annual Report seeks to help organisations and their DPOs, CPOs, CISOs and CDOs better understand why and how culture is such a significant factor in influencing the hearts and minds of employees."

The Privacy Culture team in London have compiled this research in collaboration with Queen Mary University of London, Dentons law firm, and Capgemini. We have recorded the behaviour, attitude and perceived control, knowledge and culture of over 3,000 anonymised and pseudonymised respondents, from 10 global organisations, spread across 6 industry sectors, geographically represented across 52 countries, and obtained feedback from 16 organisational functions including Marketing, HR, Customer Services and Technology.

This 2021 Global Privacy Culture Survey Annual Report is a summary of that research. It seeks to help organisations and their DPOs, CPOs, CISOs and CDOs better understand why and how culture is such a significant factor in influencing the hearts and minds of employees. The survey will monitor, benchmark and track these trends for the next 10 years.

Over the next few pages you will see our findings and recommendations according to the best and worst performing areas across our 12 key themes of data privacy, protection, security and governance and the attributes of culture, knowledge, behaviour, attitude and perceived control, as well as valuable insights by function, location and job role.

Worst Performers

Observations and Conclusion

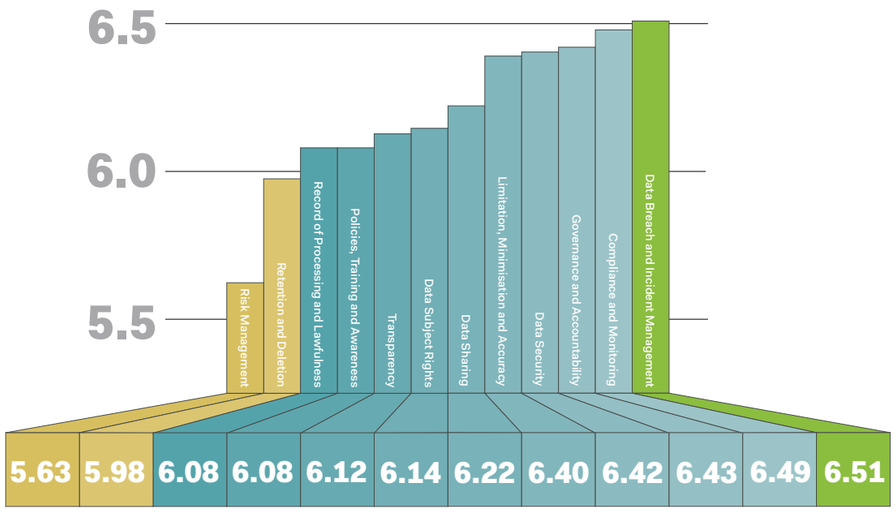
GDPR ENFORCEMENT

Regulators are continuing to fine business for GDPR infractions...

Non-compliance with general data processing principles; **Articles 5, 25, 35 GDPR.** The research clearly shows a lack of Privacy Risk Management and Privacy by Design techniques being used or implemented consistently across the workforce.

Insufficient technical and organisational measures to ensure information security (breaches) under **Article 32 GDPR.** This is Data Breach and Incident Management, and whilst the research shows this to be perceived as strong, the evidence is otherwise.

Insufficient legal basis for data processing; **Articles 5 and 6 GDPR.** Our findings also reflect this lack of understanding and adequate documentation across the research base.



2021 Benchmark
Results of the 2021 Culture Horizon survey pilot based on the average results by theme for each participating organisation

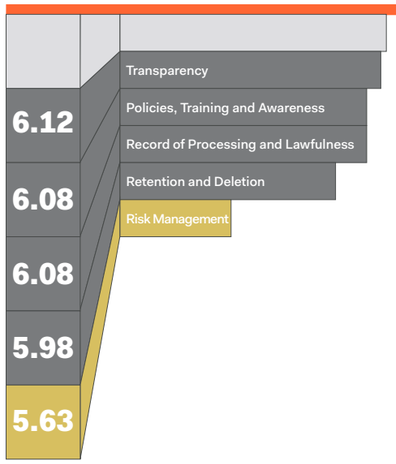
Best and Worst Performing Themes by Function

A closer look at the results by function can help to prioritise targeted training and reveal additional areas of concern that may not always emerge in the overall theme score

Function	Best Theme	Rating	Worst Theme	Rating
HR	Governance and Accountability	Satisfactory	Risk Management	Unsatisfactory
Finance	Compliance and Monitoring	Satisfactory	Risk Management	Unsatisfactory
Marketing	Data Breach and Incident Management	Inconsistent	Risk Management	Poor
Sales	Compliance and Monitoring	Satisfactory	Risk Management	Unsatisfactory
Communication	Compliance and Monitoring	Inconsistent	Risk Management	Unsatisfactory
Technology	Data Breach and Incident Management	Satisfactory	Risk Management	Unsatisfactory
Legal	Data Breach and Incident Management	Satisfactory	Retention and Deletion	Unsatisfactory
Research and Development	Data Breach and Incident Management	Inconsistent	Risk Management	Unsatisfactory
Risk and Compliance	Compliance and Monitoring	Satisfactory	Risk Management	Inconsistent
Operations	Data Breach and Incident Management	Satisfactory	Risk Management	Unsatisfactory
Customer Services	Governance and Accountability	Satisfactory	Risk Management	Unsatisfactory
Design	Data Security	Inconsistent	Risk Management	Poor
Development	Data Security	Inconsistent	Risk Management	Poor
Supply Chain	Data Breach and Incident Management	Inconsistent	Risk Management	Unsatisfactory
Property	Compliance and Monitoring	Satisfactory	Data Sharing	Inconsistent
Facilities	Limitation, Minimisation and Accuracy	Inconsistent	Risk Management	Unsatisfactory

> In theory, we undertake risk management daily but, in practice, we don't explain the how."

Worst Performing Themes
#1 RISK MANAGEMENT



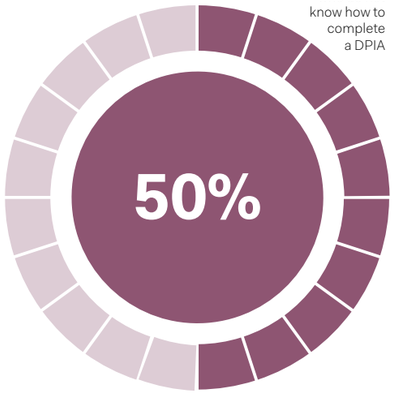
According to our research the lowest scoring results from the survey was Risk Management; despite 'risk' being mentioned over 75 times in the General Data Protection Regulation text alone.

Risk Management, particularly understanding when to complete a Data Protection Impact Assessment (DPIA) and recognising personal and sensitive personal data, consistently scored poorly across the benchmark. Almost 50% of participants stated that they would not know how to complete a DPIA for new activity involving personal data, and 26% did not know the difference between personal and sensitive personal data. This was further highlighted in the workshops where respondents remarked that the DPIA process was either unknown, or complicated, poorly communicated, or ineffective.

Attitude, behaviour, perceived control, knowledge, culture

The poor result for DPIAs could be attributed to a perceived lack of control, as many respondents felt that the organisation or DPO would know what to do and therefore they felt no personal obligation to question or identify the risks associated with processing activities, let alone the associated rights and freedoms that could be impacted by the undertaking of this activity. And, as one CISO remarked: 'Organisations often look to protect employees from certain processes in order to lessen the burden on their role'.

The inability to recognise personal or sensitive personal data is perhaps more fundamental and clearly needs to be reinforced in foundational training and awareness throughout the organisation.

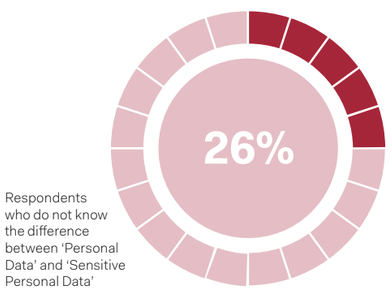


Respondents who do not know how to complete a DPIA

Findings by Function and Location

Results indicated that **Communications, Development**, and **Facilities** appear to be 'failing' in this area, and **Marketing**, **HR** and **Legal**, all scored a 'poor' result when asked if they carry out a Data Privacy Impact Assessment before starting a new project or activity that involves collecting or using personal data.

Feedback from the workshops reinforced the confusion around the purpose and use of DPIAs. Once a brief overview was provided to participants, concern was raised by them around the level of potential risk exposure occurring within organisations, as a consequence of DPIAs not being conducted or used properly.



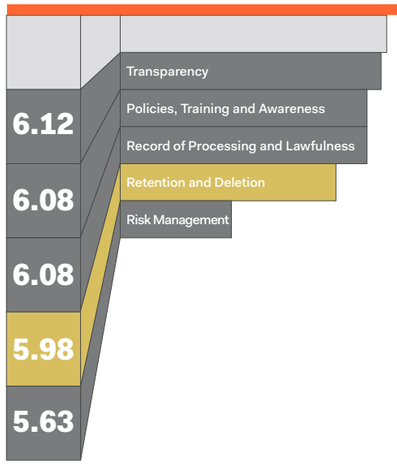
Respondents who do not know the difference between 'Personal Data' and 'Sensitive Personal Data'

Interestingly, all functions–with the exception of **HR**–seemed to believe that this was not their responsibility; this underlines the continued need for DPIA training and awareness for all parts of the organisation.

The average score for all participating countries was 'unsatisfactory' overall. Although the culture of an organisation or its attitude towards risk management may differ from one part of an organisation to another, in most cases these factors would appear not to be exacerbated by location or function.

> There is a lot of education, but it doesn't mean I understand it–there is a lack of clarity."

Worst Performing Themes:
#2 RETENTION AND DELETION



There is a clear lack of understanding and process maturity surrounding the application of data retention and deletion schedules. This problem is not isolated to one organisation, as nearly every participating organisation scored poorly in this area with 50% scoring 'unsatisfactory' overall.

Furthermore, of our participating employees:

- 38% don't know whether their organisation communicates the deletion or disposal of personal data to relevant third parties and, when applicable, to the individuals concerned.
- 28% are not confident that personal data is deleted or anonymised once it has been used for the original purposes(s) for which it was collected.
- 27% do not understand the procedure in place for the secure deletion and disposal of personal data.

The challenge of implementing and complying with data retention and deletion schedules is made more difficult by the perceived cheap cost of storage and the simplicity of purchasing or utilising cloud-based data storage. What's more, employees do not seem to have sight of what needs to happen when it comes to sharing and ensuring that the personal data entrusted to third parties is securely deleted.

Attitude, behaviour, perceived control, knowledge, culture

The data shows that nearly all the participating organisations lack sufficient communication on when, why and how personal data should be retained or deleted. This leaves employees confused and unclear on the implications of non-compliance; not understanding the fundamentals of data subject rights can lead to a hesitance to act, especially regarding the right to deletion.

Findings by Function and Location

This topic scored poorly across all functions and locations, and there was a lack of clarity around responsibility and ownership of data sets in addition to the process by which data could be deleted securely and the sign-off process required.

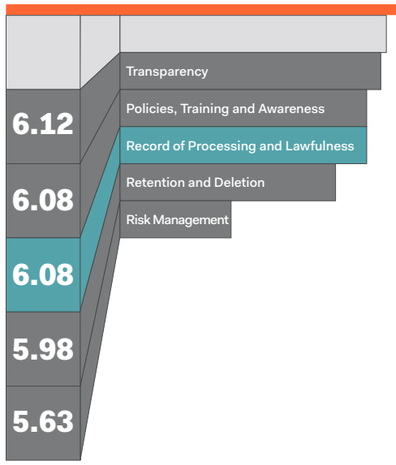
38% ...don't know whether their organisation communicates the deletion or disposal of personal data to relevant third parties or the individuals concerned.

28% ...are not confident that personal data is deleted or anonymised once it has been used for the original purposes for which it was collected.

27% ...do not understand the procedure in place for the secure deletion and disposal of personal data.

> A lot of this goes straight over my head, it needs to be communicated in a way that I understand."

Worst Performing Themes
#3 RECORD OF PROCESSING AND LAWFULNESS



Records of Processing Activities (ROPA) survey questions scored poorly with 50% of participants scored 'unsatisfactory' overall. Following the survey workshops, we can also conclude some interesting revelations that could encourage and foster a debate for both a change in perception and application of this, principally GDPR, requirement.

Attitude, behaviour, perceived control, knowledge, culture

There was a gap in employees' understanding of the usefulness and purpose of the ROPA. In the workshops, it was seen as a 'DPO problem' and, therefore, the low survey scores suggest that this lack of clarity on the role and purpose of the ROPA is not helping to promote local data ownership, accountability and responsibility. Could this be part of a wider misunderstanding about personal data transparency and accountability?

Findings by Function and Location

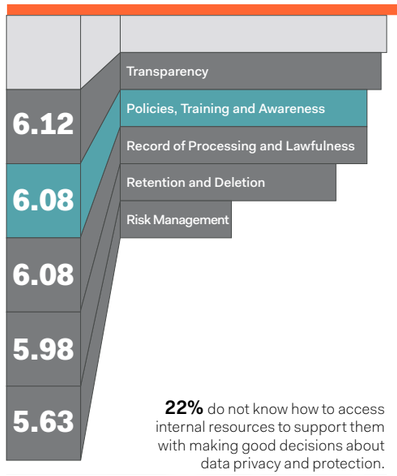
Although scores were still 'inconsistent', functions that were more confident around the existence of centrally recorded records of processing included HR, Finance, Technology, and Risk and Compliance.

Perhaps surprisingly some European locations produced an 'unsatisfactory' score despite the application of the GDPR – but this could be an indication that they are aware of what they should know – but do not currently have that knowledge.

19% of participating employees are not confident that all activities that collect and use personal data (including the IT systems used) are recorded and maintained centrally in their organisation.

> There has been an attitude shift towards the importance of personal data in the past 24 months, but we still don't understand what to do on a day-to-day basis."

Worst Performing Themes
#4 POLICIES, TRAINING AND AWARENESS



22% do not know how to access internal resources to support them with making good decisions about data privacy and protection.

21% state that the importance of data privacy and protecting personal data is not regularly discussed in their organisation.

26% of participating employees do not believe it is normal practice to talk to, or report, colleagues if they do not handle personal data in an appropriate manner.

This area not only focuses on the application of an organisation's culture, policies, and training and awareness programme; it also enables us to unravel why certain themes do not appear to be operating satisfactorily, and what might be done to resolve this.

Attitude, behaviour, perceived control, knowledge, culture

Our workshops revealed that, generally speaking, employees are aware and concerned that they lack the required knowledge to adequately manage and protect the personal data they handle on a daily basis, a reflection of the 50% 'unsatisfactory' score in the survey for this area overall.

Participants remarked that there was a lot of activity around the time of the GDPR coming into force, resulting in annual compliance training at foundation level. However, it is still difficult to understand the rules around data sharing and deletion particularly between internal and external recipients and where different mechanisms are in place. Whilst guidelines might exist, employees are often unclear which process to adopt and under what circumstances.

There also seems to be an over-reliance on the use of broad-brush communication vehicles, such as the company intranet, to communicate new procedures. Workshop participants conveyed concerns that messages would frequently be lost 'in the noise' and processes and procedures were hard to find or difficult to follow.

Findings by Function

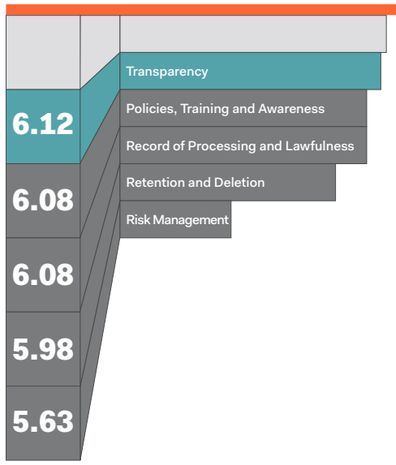
At the theme level, functions appeared to perform in a comparable way across the organisation. Also, some participating organisations were heavily weighted towards Technology, for example. In the workshop discussions it was clear that areas such as HR, Risk and Compliance and IT Security were keen to share and understand more, so there is an opportunity to invest in targeted training for these employees that they might support the DPO, and other data related areas, by acting as ambassadors or champions across the whole business.

Findings by Location

The emerging themes were again quite similar at a high level which will be helpful for the DPO when designing an awareness, education and training programme globally, however in some cases deeper analysis revealed that in smaller countries (where potentially access and authority is concentrated on a small number of individuals) even a basic understanding of data protection and privacy procedures are missing; this should be ignored at the peril of the DPO.

> When I joined the organisation, over 5 years ago, there was loads of training but now training is less and less– and yet more and more compliance box ticking"

Worst Performing Themes
#5 TRANSPARENCY



A **transparent approach** to data protection and privacy is central to effective internal and external communication. Transparency is key for data subjects to understand their rights, how their personal data is protected and who is accountable when those rights are violated.

The requirements for transparency are spelt out in GDPR Articles 12-15, requiring the organisation to detail the data processing activities in a concise, transparent, intelligible and easily accessible form, using clear and plain language; as well as providing access to any data held, when requested by a data subject.

Attitude, behaviour, perceived control, knowledge, culture

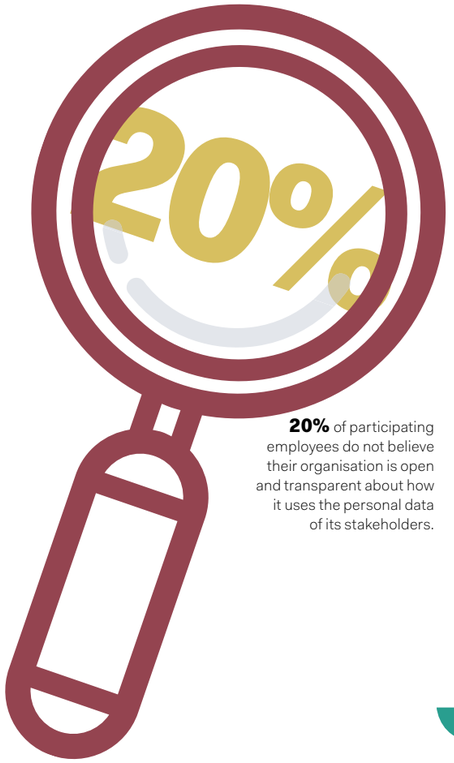
However, our survey findings show that not only are many privacy notices unclear, they could also be misrepresenting the actual processing activities being carried out within the organisation. This is not necessarily due to an organisation deliberately misleading the public, rather it is that privacy notices can be vague and non-committal, leading to more confusion about who is doing what, and with what data.

This means more queries from customers and employers are being directed to the DPO or Customer Services, rather than being answered with a comprehensive notice.

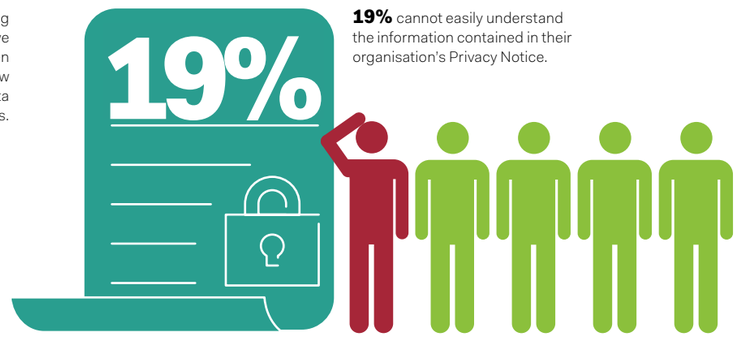
Findings by Function and Location

Although functions including HR, Customer Services, and Risk and Compliance scored better here, results were still 'inconsistent'. Perhaps surprisingly Marketing and Legal were amongst those participating employees displaying an unsatisfactory result – but again it could be that they 'know what they don't know'.

At the country level, results were a mixture of 'unsatisfactory' and 'inconsistent', with the overall average lifted in all probability by participating employees in India who scored 'satisfactory' overall – could this be a reflection of the highly educated workforce there?



20% of participating employees do not believe their organisation is open and transparent about how it uses the personal data of its stakeholders.



19% cannot easily understand the information contained in their organisation's Privacy Notice.

> Getting to know these functions will help you immensely when thinking about developing your Privacy Culture."

Observations
Function

Functions have distinct cultures, so it is pointless trying to treat them the same or expecting them to be equally responsive when it comes to engaging with your data protection and privacy activities. Spending a little time getting to know the personalities of these functions in terms of how they operate and where their pain points and pressures are will help you immensely when thinking about developing your Privacy Culture.

Function	Governance and Accountability	Limitation, Minimisation and Accuracy	Retention and Deletion	Transparency	Records of Processing and Lawfulness	Risk Management	Data Security	Policies Training and Awareness	Data Sharing	Data Subject Rights	Data Breach and Incident Management	Compliance and Monitoring
HR	↑	↗	→	↗	↗	→	↗	↗	↗	↗	↗	↑
Finance	↑	↗	↗	↗	↗	→	↗	↗	↗	↗	↑	↑
Marketing	↗	↗	→	→	→	↙	↗	→	→	↗	↗	↗
Sales	↗	↑	→	↗	→	→	↗	↗	↗	↗	↑	↑
Communication	↗	↗	→	→	→	→	↗	→	→	→	↗	↗
Technology	↗	↗	↗	↗	↗	→	↑	↗	↗	↗	↑	↑
Legal	↗	↗	→	→	→	→	↗	→	→	↗	↑	↗
Research and Development	↗	↗	↗	↗	↗	→	↗	↗	↗	↗	↗	↗
Risk and Compliance	↑	↑	↗	↗	↗	↗	↑	↗	↗	↗	↑	↑
Operations	↗	↗	↗	↗	↗	→	↗	↗	↗	↗	↑	↗
Other	↗	↗	→	→	→	→	↗	→	↗	→	↗	↗
N/A	↗	↗	↗	↗	→	→	↗	↗	↗	→	↗	↗
Customer Services	↑	↑	↗	↗	↗	→	↗	↗	↗	↑	↑	↑
Design	↗	↗	→	→	→	↙	↗	→	→	→	↗	↗
Development	↗	↗	→	→	→	↙	↗	→	→	→	↗	↗
Supply Chain	↗	↗	↗	↗	↗	→	↗	↗	↗	↗	↗	↗
Property	↑	↑	↗	↗	↑	↗	↗	↗	↗	↗	↑	↑
Facilities	→	↗	→	→	→	→	→	→	→	→	↗	→

The next step in obtaining engagement from your functions is planning. And this is where it is helpful to leverage your diverse team. Your programme and change manager will be across this already and thinking about the optimum time to start an activity with HR and Finance for example–and which times should be avoided.

One of the best ways to educate your Communications and Marketing teams is to draw on their own skills and creativity to help them educate themselves and the entire workforce. Do not try and impose new channels or ways of working on them. They own this space and will be way ahead of you, so take their lead and eventually it will pay dividends as they will be some of your biggest supporters.

We noticed from our survey results that Communications sometimes scored a little lower in knowledge and confidence in all areas of Data Protection and Privacy, Security, and Governance. We are all missing a trick here as ensuring the Communications function have a high awareness of the topic –and strong engagement with your team and your programme– will mean that it is more likely to be promoted on the back of other company-wide campaigns at every opportunity, you will get the front page of the intranet to promote your training, and they will hold the front page for you on 28th January for Data Privacy Day!

Performance by Function
Cross-referencing how each function scored overall across each of the 12 maturity domains:

↑ Satisfactory ↗ Inconsistent
→ Unsatisfactory ↙ Poor

Observations
Sector

> Sectors that are data-intensive and perhaps more used to regulation, appear to be at an advantage when embedding their culture of compliance."

We are now able to look at and understand the differences between industry sectors, to try and understand which naturally perform better than others when it comes to privacy. For this exercise, we have grouped our organisations into the sectors of Finance, Data Services, Charity, and Consumer Services.

This approach has provided us with a broad view of organisations operating across very different environments, with very different clients, structures and general operating parameters. What becomes immediately–and perhaps unsurprisingly–clear is that the Data Services and Finance sectors perform well. That's not to say that these two sectors were more mature than the other sectors as all rated as 'inconsistent'.

However, sectors that are data-intensive and perhaps more used to regulation, appear to be at an advantage when embedding their culture of compliance, compared to organisations such as the Consumer Services sector where privacy frameworks appear less mature.

Nevertheless, for common areas of challenge such as Risk Management and ROPAs, all sectors were seen to struggle to an almost equal degree; but for areas such as Policies, Awareness and Training, and Retention and Deletion, this appeared to be more pronounced within the Consumer Services sector.

The data does show a consistency of scoring across sectors which, in turn, supports the fact that many of the challenges to operating a successful privacy framework are not sector-specific but more culturally based. Accordingly, organisations should look to focus on informing the attitudes, knowledge and behaviours of employees in order for them to be able to carry out the correct actions on a repeatable basis.

Focus should be put on ensuring the policies are in place to support the learnings around data sharing, the use of DPIAs to understand and mitigate risks, the differences between personal and sensitive data and the period for which data should be kept. These are the activities that will help improve privacy frameworks, irrespective of the sector in which a company operates.

Observations
Region

> Risk Management, Retention, Training and Awareness, ROPAs and Transparency are consistently under-performing across our regional spread"

From a regional perspective, we can see that progress is being made across Europe, USA, Canada, Australia, Japan and other developed economies, but there is still a lack of maturity across less regulated countries or jurisdictions where data protection and privacy can be perceived, handled and managed in a less prescriptive, more libertarian manner.

APAC ASCENDANT
Asia Pacific gave a very strong response in the first survey, helped in no small part by India.
The Americas, however, were pulled down somewhat by Canada's relatively 'unsatisfactory' response.

Interestingly we noticed that some European countries were scoring themselves lower than in regions where privacy and data protection laws are emerging or non–existent. This could indicate a higher maturity, in so far as they are aware of what they don't know, but remedial action is not taken.

We can see from the results that the areas of Risk Management, Retention, Training and Awareness, ROPAs and Transparency are consistently under-performing across our regional spread. This is partly due to countries operating differing privacy regulations and enforcement regimes, but also cultural differences in employee behaviour and attitudes towards privacy and in the way they respond to surveys - although on balance it amounts to the same themes.

This regional attitude was even apparent in our survey participation figures; we noticed that many countries producing stronger results had higher employee response rates. However, if the maturity of country's adoption of privacy law or regulation is low, then the start point from which employees are answering these questions are also naturally low – especially in comparison to countries with greater knowledge and more mature data protection requirements i.e. European countries. This makes sense but does beg the question that perhaps some of these seemingly robust global average scores might not be as positive as they at first appear for our first global GPCS 2021. We will come back to this next year and see if there has been an uplift in the benchmarked scores globally.

Highest Mean Regional Score: India

6.59
Satisfactory
509 Participants
Regional Score: **6.40**

Special Relationship: UK and USA

USA **6.23** VS UK **6.18**
Inconsistent
423 + 1,038 Participants

Lowest Americas Mean Score: Canada

5.78
Unsatisfactory
244 Participants
Regional Score: **6.09**

Observations
Role

> Although the GDPR states the DPO should have expertise in data protection law and practice, it does not stipulate the role should be held by a lawyer."

Industry is now beginning to recognise that a balanced composition of the data protection function will provide the best results.

This approach could mean utilising those who may not necessarily have a background in data protection, law, privacy or security, but who are excellent communicators, networkers, programme and resource managers. This diverse team also needs to be supported by privacy allies or champions across all business functions.

Although the GDPR states the DPO should have expertise in data protection law and practice, it does not stipulate the role should be held by a lawyer. However, most organisations that employ a DPO often insist they have a background in law and will therefore have a strong technical understanding of Data Protection and Privacy requirements that work well for policy and contract writing but not necessarily for communicating important concepts such as What Personal Data Is, How to Identify and Report Data Rights Requests, and How to Identify and Report a Data Incident.

We need to remember that the workforce we are trying to educate is likely to be diverse and disparate with different and, potentially, opposing sub-cultures, priorities, pressures, and have varying levels of knowledge and behaviour around data protection and privacy, security, and governance.

This year, we have identified variations in attitudes across sectors, functions and roles. This can be attributed to the maturity of the privacy and security awareness and training programme as well as the visibility and simplicity of processes and other resources i.e. champions to support the messaging. Our workshops identified individuals at certain levels of the organisation who were incredibly enthusiastic about privacy and its importance, even if they were not always sure what to do in practice.

There is an opportunity to leverage these enthusiasts as champions, for example taking advantage of seniority to promote the importance of data protection and privacy amongst leadership peers and to up-skill individuals to help embed important concepts, such as risk management, at a local level.

The ability to train and re-enforce key privacy concepts as well as the more technical aspects of privacy and data protection is crucial to building your privacy culture from the ground up. Employing creative individuals with a capacity for articulating information often seen as boring and tedious, as well as harnessing existing communication channels that are known to be effective, is essential to achieving the level of confidence and compliance you seek.

Conclusion
Why data protection and privacy cultures matter in the workplace

It has been said that an organisation is only as good as the people who work there, and this is reflected in its culture, products and services.

It could be argued that GDPR has led to wide-spread global data protection and privacy uprising, with organisations around the world recognising the value of good data governance. Of course, the less glamorous impact has been the very different privacy practices that have emerged globally, with both organisations and enforcement agencies slightly interpreting these principles differently and therefore as a result – differing ways of how compliance can and should be achieved.

The DPO has the responsibility to interpret these privacy rules and then apply them to his or her business environment or organisation. This has led to wide-spread differences and quality in interpretation and implementation, but yet one common challenge remains outstanding – 'how to embed a culture of privacy across the workforce'. How do you inspire employees to behave and act differently when it comes to personal data handling and access? How do you make privacy interesting to employees? How do you turn it into one of the organisation's values?

A focus on compliance at the expense of culture could mean a restricted view of a prospect or customer for a salesperson, which would, in turn, impact conversion rates and profitability. It could cause confusion for employees wishing to understand their target customers better, given their lack of understanding about what can and can't be done with personal data. Yet organisations have spent millions on collecting terabytes of valuable and insightful customer behaviour data, and yet they have failed to realise the true value of that data because they have not simultaneously addressed the culture of privacy within their organisation. Our survey research also shows this to be reflected consistently across different jurisdictions, sectors, functions and even the different roles that took part in the survey.

The results of this study indicate that organisational culture mainly impacts motivation, promotes individual learning, affects communication, and improves organisational values, group decision making and solving conflicts. If we are ever to move the conversation to how personal data can add business value, drive stronger revenue growth, help margin expansion and drive data utilisation, then we will need to move away from 'tick box' notions of data protection and privacy compliance, abandon the scare tactics of non-compliance, and even stop worrying so much about fines from regulators.

CLOSING THOUGHTS

Do not expect the procurement of more privacy compliance software to solve your privacy culture problems.

Enhance the business value proposition by utilising datasets in accordance with their lawful purposes and the value they bring to the organisation; be honest and open with your workforce and customers.

Empower the workforce by driving through pragmatic, relevant, appropriate privacy tools and bespoke knowledge training; not by eLearning alone and not through Death-By-PowerPoint.

Embed Privacy By Design techniques before you start building products or go live with consumer-accessible applications or ventures.

Facilitate a privacy culture that rewards good data ethics and governance.

Make transparency your business goal, and charge marketing colleagues to act as custodians of this initiative; nominate board members to own data sets.

Give your employees a voice and ask for their opinions on the way to achieve data protection and privacy; utilise the Culture Horizon tool to survey employees' views.

Global Privacy Culture Survey 2022

You have now seen the results of our first year's global privacy culture survey, but the vital work continues as, every week, new organisations sign up to find out more about their employees' attitudes and behaviours.

Culture Horizon is the powerhouse behind the Global Privacy Culture Survey. Its 7-point Likert scale telemetry is collected on secure UK-based servers before being analysed by our experts and then collated into bespoke user reports and presentations.

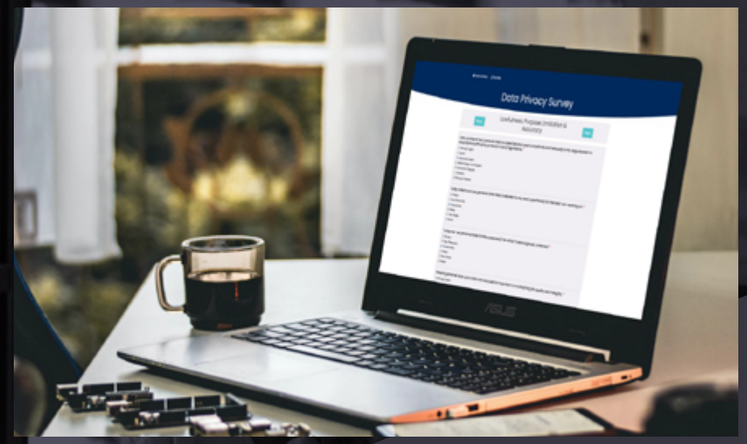
3K+
anonymised respondents

52
nations participating

31%
invited employees who completed the survey

16
business functions polled in the survey

10
organisations in our 2021 pilot



The average completion time for our survey is 14.5 minutes, in which time employees will anonymously answer 50 opinion-style questions that give insights into their Behaviour, Knowledge, Attitude, Perception of Control and the Organisational Culture.

April 2021 saw the start of our next year of data gathering. Every Culture Horizon survey carried out between then and March 2022 will add more depth, insight and comparison data to our next Annual Report. We'll be tracking how all of the issues raised and covered here are progressing: are we looking at industry-wide trends? Are there global issues that we need to be concerned about? Are we seeing improvement in those companies polled in previous years?

As well as the ability to compare organisations against their peers, what else do participants gain from the survey? Behind the broad-spectrum numbers you've read here, are bespoke and far-reaching reports into the privacy culture of those companies taking part. Our data analysts have already carried out full debriefing sessions with all our participants. They have been presented with personalised reports containing summarised, analysed and visualised data for them to digest and begin the task of making those changes that will lift scores and bring improvements to behaviours and attitudes. Where applicable, we have outlined clear and pragmatic guidance to remediate problem areas identified over the course of the survey. We look forward to repeating the process over the coming year and reporting back on the progress that they–and the industry as a whole–has made.

The participant feedback so far has been overwhelmingly positive with one organisation reporting *"this is so powerful–it turns my strategy on its head"* and another claiming that *"after completing the survey my GC wants to roll out the Privacy Culture Survey regularly"*.

With a range of packages to suit all organisation sizes and locations, the Culture Horizon survey is now open and available to you. Our team of data scientists, analysts and privacy lawyers are ready to partner with you to map out your organisation's culture of privacy and begin making those improvements that you may have suspected but could never prove were needed.

Call us now on **+44 (0) 20 7112 9360**
Email us at **Hello@PrivacyCulture.com**
Or complete the simple form at **PrivacyCulture.com/Survey**

Appendix: The 12 Domains

The **Culture Horizon** survey is underpinned by the same **12 domains of privacy and data protection** that form the backbone of our proprietary **Maturity Horizon** assessment. These domains are mapped to existing and emerging global privacy and data protection laws.

Governance and Accountability

The organisation has appropriate levels of accountability, a defined organisational structure and responsibilities are known and understood at all staff levels.

The organisation has a Privacy Team in place supported by a network of Privacy Champions. There is an adequate governance structure in place with appropriate Board level oversight including Audit and Risk Committee representation.

Limitation, Minimisation, and Accuracy

Data processing meets the legislative standard of 'purpose limitation', 'data minimisation', and 'accuracy'. **[Article 5, 1(b-d)]**

Key processes and operations are in place to ensure controls and safeguards are adequate and monitored.

Retention and Deletion

Personal data is processed by the organisation for no longer than is necessary for the purposes for which it was collected. **[Article 5, 1 (e)]**

Deletion procedures are in place and regular back up includes appropriate provision in order to comply with relevant and localised privacy, repatriation and employment laws.

Transparency *(Privacy and Cookie Notices)*

Current, accurate, relevant and communicated privacy and/or cookie notices for all business processes.

Adequate and clear guidance for customers and employees to follow for further information or rights enquiries.

Records of Processing and Lawfulness

The organisation's Record of Processing complies with data protection regulations and is comprehensive, accurate, current and accessible. **[Article 30, Article 5 (2)]**

In particular, the lawful basis is adequately described and explained.

Risk Management

There is a documented procedure for managing privacy risks that applies across the organisation.

Managing privacy risk including a definition of the organisation's risk appetite and how to conduct privacy risk impact assessments using a structured and systematic approach to risk assessment including recording, monitoring and reporting risks to the appropriate committee or Board member or Risk Officer.

Data Security

The organisation and its processors have implemented technical and organisational security controls to ensure an appropriate level of security is considered and applied across the people, process and technology. **[Article 5 (1f), Article 32]**

Data Protection by Design and Default is embedded into all organisation change systems, business change request system including logging, monitoring and tracking of the DPIA process. **[Articles 25 and 35]**

Policies, Training and Awareness

The organisation has data protection policies and procedures in place and that all employees are familiar with the policies and have received adequate and appropriate role-based data protection training.

This includes a clear communication, awareness and training programme that is rolled out, measured, monitored and evaluated for effectiveness.

Data Sharing *(Third Parties)*

The organisation has contracts in place with internal and external data processors; the data processors have provided guarantees to implement technical and organisational measures to comply with data protection regulations

Sub-processors are not used without the organisation's written authorisation and data sharing agreements are in place and regularly reviewed. **[Article 28 and 29.]**

Rights

Data Subject Rights at the organisation are supported by adequate processes and procedures in place.

Systems and procedures are operational and embedded to manage both personal data and data subject rights requests.

Data Breach Management

Data breach and Incident Management is carried out in accordance with data protection regulations in country and that appropriate guidelines are available to all staff and stress testing is conducted regularly. **[Articles 33-34]**

Compliance and Monitoring

The organisation has a data protection compliance (control) framework, which demonstrates adherence with relevant laws and regulations.

The organisation monitors personal data handling and regularly conducts internal and external audits. Annual privacy compliance testing and reporting to the Board is operational.

PrivacyCulture.com

Bouverie House | 154-160 Fleet St | London | EC4A 2DQ
T. +44 (0) 20 7112 9360 | Hello@PrivacyCulture.com

CREDITS

PCL// **Nichola Sudweeks** / Culture and Change Manager; **Rhys Walden** / Privacy Analyst; **Kimberley Watts** / Office Manager; **Christos Zimaras** / Training and Awareness Manager.
KICKTAG// **Pete Ansell** / Founder; **Jack Putt** / Software Development Manager
PICTURES// **Architecture** / Joakim Nadell / Luca Bravo / Simone Hutsch / Unsplash
DESIGN & PRODUCTION// mistereb.com

GLOBAL
PRIVACY
CULTURE
SURVEY