

# Learning Hub

**Data Protection, Digital and Technology**

**2024 Regulatory Developments**



# Contents

<b>1. High Volume Data Access Requests</b>	<b>3</b>
<hr/>	
<b>2. The Data Protection Commission 2023 Annual Report</b>	<b>7</b>
<hr/>	
<b>3. Further Insights on the DPC's 2023 Annual Report</b>	<b>14</b>
<hr/>	
<b>4. Empowering employees with AI chatbots</b>	<b>22</b>
<hr/>	
<b>5. Navigating Legitimate Interests Assessments</b>	<b>26</b>
<hr/>	
<b>6. International Data Transfers</b>	<b>30</b>
<hr/>	
<b>7. The 5 Most Common Data Privacy Mistakes of 2023 (and How to Prevent Them)</b>	<b>33</b>
<hr/>	
<b>8. Refresher on Legal Basis</b>	<b>36</b>
<hr/>	
<b>9. Black Friday is Almost Here. Is Your Marketing Campaign Compliant?</b>	<b>39</b>
<hr/>	

# High Volume Data Access Requests

Date of issue: 24 May, 2024

# High Volume Data Access Requests

**Under the GDPR, data subjects have the right to request access to the personal data that an organisation holds about them. It can be difficult for organisations to respond to high volume data access requests.**

In some cases involving significant amounts of personal data, a data subject access request (DSAR) made under the GDPR can bring the daily operations of a business to a standstill.

In this article, to help you streamline your DSAR process and minimise the impact to your day-to-day business, we take a look at some of the key points to consider when managing and responding to DSARs.

## High Volume DSARs

Under the framework of the GDPR, organisations are responsible for honouring an individual's right to access their personal data.

A data controller has up to one month to respond to an access request (extendable under limited circumstances). The scope and complexity of DSARs can vary greatly, and the request can originate from different data subjects such as employees or customers.

Where, for example, an access request comes from an employee with many years of service, it might involve retrieving, reviewing, and redacting high volumes of data. Further, as prescribed by the GDPR, this must be done to an accurate standard and within the statutory deadline.

## Streamlining the DSAR process

There are a number of ways to streamline the DSAR process to ensure a timely and accurate response to a request, thereby reducing exposure to fines and reputational damage, and diverting crucial resources back to core business functions.

### **Technology solutions and automation:**

Advancements in technology are revolutionising DSAR management, offering innovative solutions to streamline processes and enhance efficiency. Data analytics tools and automation software can accelerate response times, reduce manual effort, and improve overall data governance practices.

# High Volume Data Access Requests

## High Volume DSARs cont.

Failure to comply not only violates regulatory requirements but also exposes businesses to significant legal and financial risks, as well as potential reputational damage.

“In responding to a request, often an all-hands-on-deck approach is necessary: input from the HR team, the IT team, in-house legal, and senior management may all be required” says Emma Ritchie, head of data protection and privacy at KPMG Law.

“This can be a huge drain on resources, and the sheer volume and complexity of data can overwhelm internal teams and hinder operational efficiency”, Ritchie adds.

## Streamlining the DSAR process cont.

“By leveraging technology solutions, businesses can stay ahead of the curve and adapt to evolving regulatory requirements while optimising resource utilisation” states Andy Glover, Director in KPMG Managed Legal Solutions.

### **Get proactive:**

Proactive data management strategies are essential for minimising the impact of DSARs on business operations. These include implementing data minimisation policies, maintaining comprehensive records of personal data, and providing regular training to employees on DSAR handling procedures. By taking a proactive approach to data management, you can better anticipate and manage DSARs, and ensure compliance while maximising operational efficiency.

# High Volume Data Access Requests

## How we can help

As specialised service providers, KPMG Managed Legal Solutions together with KPMG Law offer invaluable support in navigating the complexities of DSARs. We utilise market leading AI integrated technologies to support your organisation throughout the response process.

Our team of dedicated document review specialists are on hand to relieve the resource burden and provide expert and cost-effective advice. Dovetailing with this, KPMG Law provides holistic legal advice and supports communications with data subjects and the supervisory authorities as required. We know every business is unique, so whether you are a small business or an enterprise level organisation, our solution is scalable to accommodate your needs.

## Future trends and regulatory developments

Finally, looking ahead, it's important for all organisations to keep up to speed with emerging data privacy trends and regulatory developments.

From changes to the GDPR, to evolving consumer expectations, international data transfer rules, (and the imminent impact of the new European AI Act), many factors will continue to shape the landscape of DSARs.

By staying informed and proactive, you can ensure your business successfully adapts to regulatory changes, positioning you for long-term success in an increasingly complex regulatory environment. Keep an eye on our website and LinkedIn for regular data protection and privacy updates or contact our KPMG Managed Legal Solutions team or our KPMG Law team directly.

# The Data Protection Commission 2023 Annual Report

Date of issue: 29 May, 2024

# The Data Protection Commission

## 2023 Annual Report



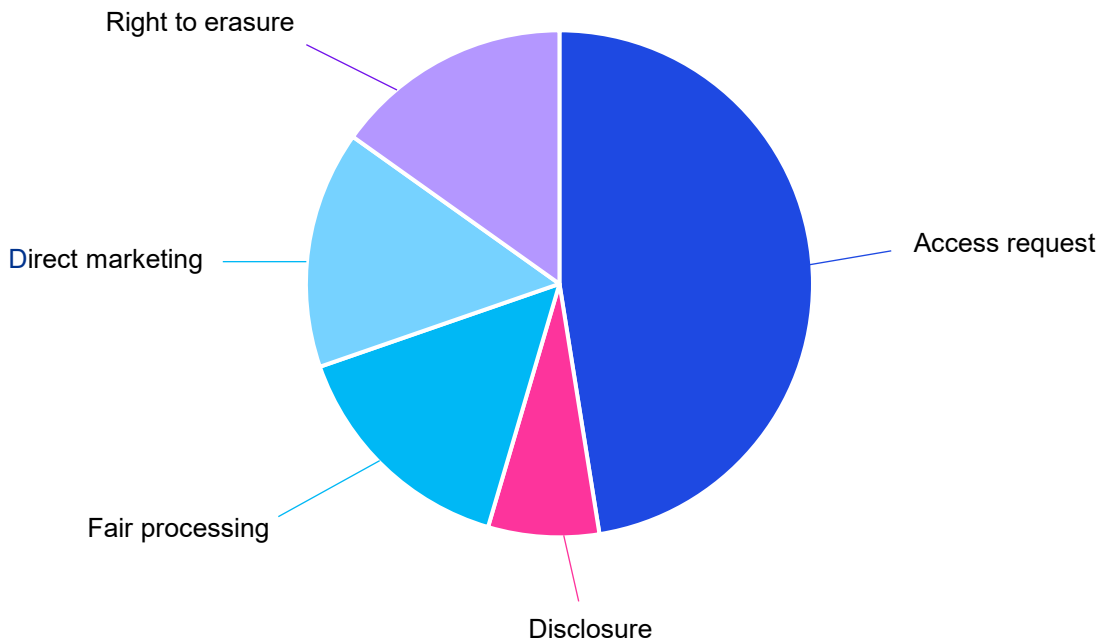
On 29 May 2024 the Data Protection Commission (“DPC”) released its 2023 annual report. The DPC highlighted its workload and regulatory accomplishments over the last year, including the finalisation of 19 decisions that yielded fines totalling €1.55 billion, along with multiple reprimands and compliance orders being processed.

### Contacts, Queries and Complaints

Between 1 January 2023 and 31 December 2023, the DPC:

- Received 25,130 electronic contacts, 7,085 phone calls and 1,253 postal contacts;
- Received 11,200 new cases (an increase of 1,830 on the 2022 case figures and the most cases received by the DPC in any year since the GDPR took effect) of which 2,600 progressed to the formal complaint handling process;
- Concluded 3,218 complaints, including 1,756 complaints received prior to 2023.

### Top 5 categories of complaints received under the GDPR in 2023





# The Data Protection Commission

## 2023 Annual Report

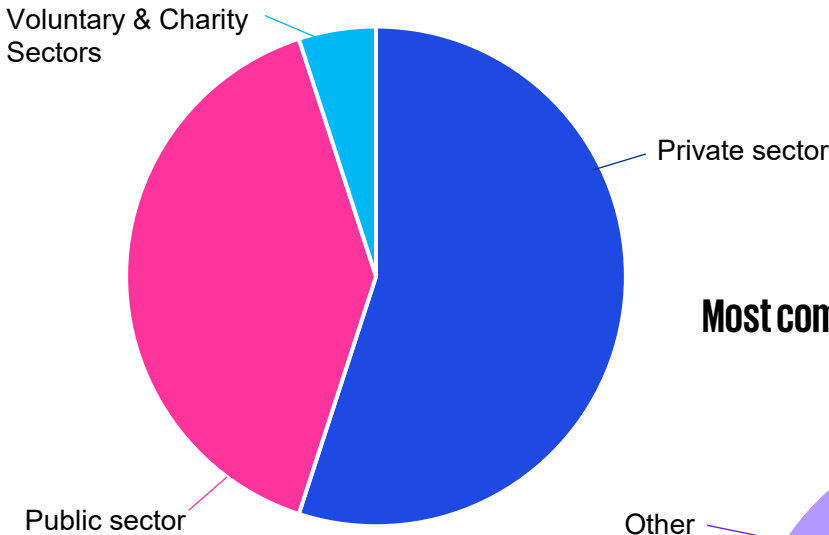
### Data Breach Notifications

The DPC received 6,991 valid GDPR data breach notifications in 2023, an increase of 20% on the GDPR data breach numbers reported in 2022. The highest category of data breaches notified to the DPC in 2023 related to unauthorised disclosures, in cases affecting one or small numbers of individuals.

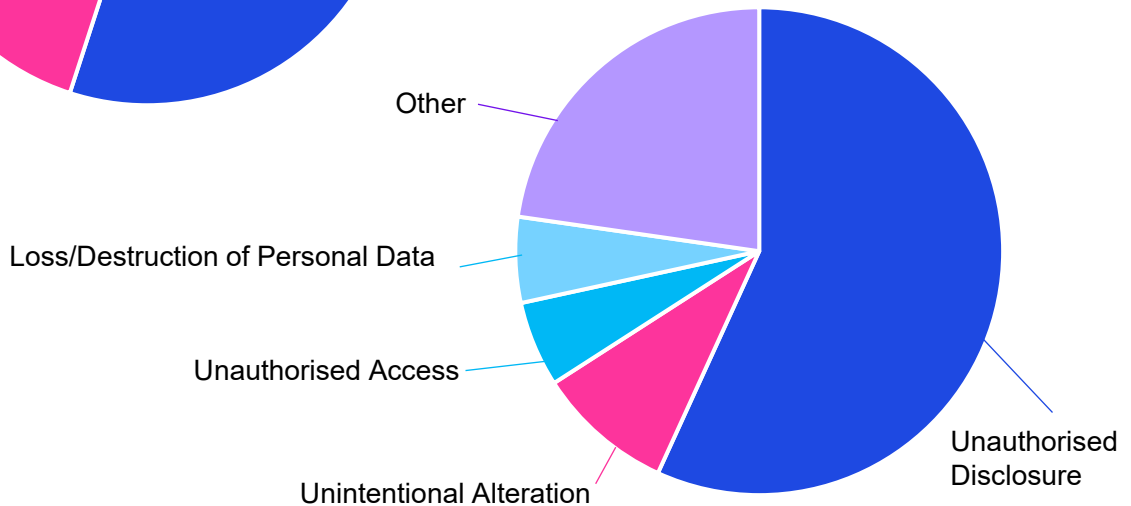
Of the 6,991 breach notifications, 3,776 related to the private sector, 2,968 to the public sector and the remaining 257 came from the voluntary and charity sectors. Public sector bodies and banks accounted for the 'top ten' organisations with the highest number of breach notifications recorded against them, with insurance and telecom companies featuring prominently in the top twenty. 92% of notifications received in 2023 were concluded by year end.

### Categories of data breach notifications received in 2023

#### Personal Data Breaches by Sector



#### Most common Personal Data Breaches in 2023



Of note, personal data breaches due to unauthorised disclosure were mainly due to posting of material to incorrect recipients or emailing incorrect recipients.

# The Data Protection Commission

## 2023 Annual Report

### Inquiries and Related Enforcement Action

The DPC issued 19 finalised decisions resulting in administrative fines totalling €1.55 billion, alongside reprimands and orders, including against companies in the technology, financial services, and healthcare sectors as well as a number of governmental entities.

Some of the most noteworthy corrective measures and fines issued as part of these decisions are:

Sector	GDPR Obligation Infringed	Corrective measures imposed	Fine (€)
Technology	<p>Article 6(1) – The company was found not to be entitled to rely on the contract legal basis for the delivery of service improvement and security and personal data processed in reliance on the contract legal basis amounted to a contravention of Article 6(1).</p> <p>Article 5(1) - The company was also found to be in breach of its transparency obligations pursuant to Article 5 GDPR by not clearly outlining to users the legal basis relied on for processing.</p>	Order regarding Articles 5(1)(a) and 6(1) GDPR	5.5 million
Technology	Article 46(1) – The company was determined to have transferred personal data from the EU/EEA to the US without a lawful basis.	Suspension of data flows in relation to Article 46 GDPR and Order regarding Article 46 GDPR	1.2 billion
Technology	Articles 25(1), 25(2) and 5(1)(c) – the company was determined to have failed to implement appropriate technical and organisational measures to ensure that, by default, only personal data which were necessary for the company’s purposes of processing were processed; and to ensure, by default, that the social media content of child users was not made accessible to an indefinite number of persons without the user’s intervention.	Reprimand regarding Articles 5(1)(a), 5(1)(c), 12(1), 13(1)(e), 24(1), 25(1) and 25(2) GDPR and Order regarding Articles 5(1)(a), 5(1)(c), 12(1), 13(1)(e), 24(1), 25(1) and 25(2) GDPR.	345 million

# The Data Protection Commission

## 2023 Annual Report

### Inquiries and Related Enforcement Action

Sector	GDPR Obligation Infringed	Corrective measures imposed	Fine (€)
Technology (continued)	<p>The company was also found to have infringed Article 24(1) GDPR by failing to implement appropriate technical and organisational measures as it related to the privacy settings of children’s user accounts and the risk of children under 13 accessing the social media platform.</p> <p>Article 13(1)(e) – the company was determined to have failed to provide child users with information on the categories of recipients of personal data.</p> <p>Article 12(1) – the company was found to have failed to provide child users with information on the scope and consequences of the public by default processing in a transparent manner.</p> <p>Articles 5(1)(f) and 25(1) – the DPC stated that the company was in breach of these articles by allowing an intended Parent/Guardian to enable direct messages for a child user where such messages were not previously enabled by the child user.</p>	<p>Reprimand regarding Articles 5(1)(a), 5(1)(c), 12(1), 13(1)(e), 24(1), 25(1) and 25(2) GDPR and Order regarding Articles 5(1)(a), 5(1)(c), 12(1), 13(1)(e), 24(1), 25(1) and 25(2) GDPR.</p>	345 million
Governmental	<p>Articles 5(1)(c), 6(1), 6(4) and 9(1) – breach of the requirements to ensure data minimisation and lawful basis for the processing of special category data. It was found that the entity processed information in a way that was excessive and disproportionate to the aims pursued and not necessary in relation to 29 litigation files (for which there was no lawful basis for this processing).</p> <p>Article 14 – transparency. The entity did not include details of its practices in its privacy notice.</p>	<p>Ban on processing regarding Articles 5(1)(c), 6(1), 6(4) and 9(1) GDPR and Reprimand regarding Articles 5(1)(c), 5(1)(f), 6(1), 6(4), and 32(1) GDPR</p>	22,500

# The Data Protection Commission

## 2023 Annual Report

### Inquiries and Related Enforcement Action

Sector	GDPR Obligation Infringed	Corrective measures imposed	Fine (€)
Governmental (continued)	Articles 5(1)(f) and 32(1) – security of data processing. The entity should have ensured that better internal access restrictions to files were in place.	Ban on processing regarding Articles 5(1)(c), 6(1), 6(4) and 9(1) GDPR and Reprimand regarding Articles 5(1)(c), 5(1)(f), 6(1), 6(4), and 32(1) GDPR	22,500
Financial services	Articles 5(1)(f) and 32(1) – the company was found in breach of these articles in respect of the unauthorised disclosure of personal data, including financial data, on a banking app.	Reprimand regarding Articles 5(1)(f) and 32(1) GDPR and Order regarding Articles 5(1)(f) and 32(1) GDPR	750,000

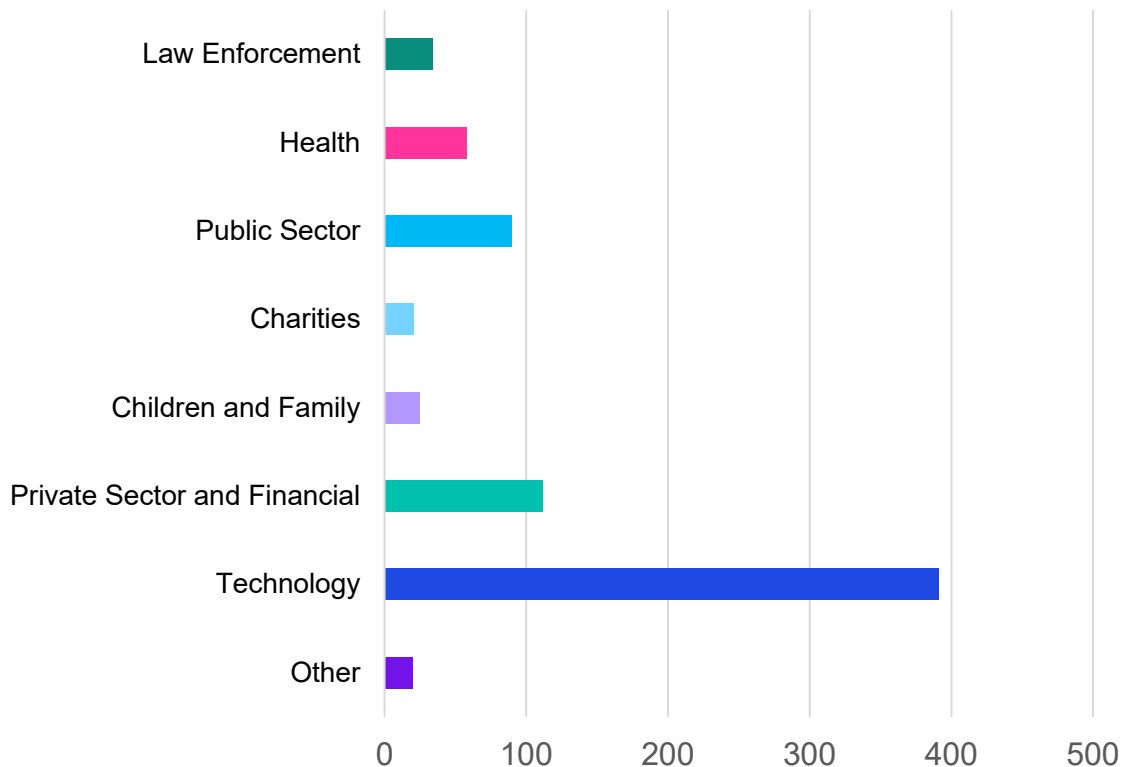
# The Data Protection Commission

## 2023 Annual Report

### Supervisory engagement

The DPC had 751 supervision engagements during 2023.

#### Supervision Engagement by Sector



#### Ongoing inquiries

As of 31 December 2023, the DPC has 89 statutory inquiries on hand, including 51 cross-border inquiries. In 2023, 18 draft decisions were referred to the EU co-decision making process (pursuant to Article 60 GDPR).

#### Funding the “New” DPC

The DPC was voted a budgetary allocation of €26.364 million in 2023, which represents a €3.1 million increase on 2022. The DPC also increased its staff numbers by 44 in 2023, bringing the total number at year end to 210.

In addition, in November 2023, Helen Dixon announced that she would step down from her role on 19 February 2024. On 20 February 2024, two new commissioners commenced their roles, Dr. Des Hogan, who serves as Chairperson, and Mr. Dale Sunderland. They will each serve a five-year term.

# Further insights on the Data Protection Commission's 2023 Annual Report

An analysis of the key themes of the report

---

14 June 2024

# Further insights on the DPC's 2023 Annual Report

To provide further insight into the approach of the DPC, we take a closer look at some of the key topics and themes noted by the DPC throughout the Report.

## Amicable Resolutions

The Report notes the important role of the amicable resolution process as part of the DPC's handling of complaints and shows the willingness of the DPC to facilitate this process.

Under the Data Protection Act 2018, the DPC must consider whether a complaint can be amicably resolved within a reasonable period. If the DPC believes an amicable resolution is reasonably likely, then it can take appropriate steps to facilitate this.

When complaints arise, data controllers should bear in mind the readiness of the DPC to initiate the amicable resolution process depending on the facts of the case.

The Report notes that in the DPC's experience a high proportion of complaints are amenable to amicable resolution in a timely fashion, benefitting both data controllers and data subjects. Interestingly, when assessed against the tendencies of other supervisory authorities across the EU, the DPC has concluded significantly more complaints by way of amicable resolution.

In 2023, the DPC resolved 578 complaints through the amicable resolution process.

# Further insights on the DPC's 2023 Annual Report

## Demonstrating accountability

The report focuses on data protection awareness, specifically certain sectors that might have certain issues arising from privacy, including the sports sector. The DPC will release a survey to key sports organisations to understand their key struggles. Organisations should review the survey to identify the key areas and ensure their data protection framework is robust enough, specifically around transparency and the collection of special categories of data such as health data.

## Data Protection Officers

The DPC has been notified of the designation of 3,520 data protection officers (“DPOs”) as of the end of 2023.

The Report, as well as the DPC’s Regulatory Strategy 2022-27, recognises the crucial role that DPOs play in championing data protection in their organisations.

The Report highlights that the DPC is committed to supporting DPOs, and often engages directly with DPO networks. Further, 2023 saw the DPC conduct a fact-finding exercise for the purpose of participating in discussions in relation to the European Data Protection Board’s Coordinated Enforcement Framework concerning DPOs.

During this review, the DPC found substantive issues in three areas:

- 1. Resources:** the Report noted that approximately 33% of respondents replied that they do not have the resources sufficient to fulfil the role of a DPO.



# Further insights on the DPC's 2023 Annual Report

## Data Protection Officers

**2. Conflicts of interest** concerns under Article 38.6 of the GDPR.

**3. Tasks of the DPO:** approximately 36% indicated that the data protection officers' tasks are performed in addition to other tasks, but not as the main task. In that regard it was noted that many of the non-data protection tasks did not compliment the role of a DPO such as Health and Safety Officer, Human Resource Officer, Employee Engagement Manager, Communications Officer.

Organisations should ensure that DPOs are well supported and resourced, and the tasks of the DPO are appropriate and proportionate to the role. Articles 37 – 39 of the GDPR are instructive in this regard, and given the significance of the role, it is vital that DPOs have the expert data protection knowledge required to perform their tasks and are not distracted from this task by other compliance roles.

## Children's data protection rights

Children's data protection rights are a priority focus area for the DPC.

This is apparent from the spotlight on children's rights in the Report, and the inclusion of the topic as a main focus in the DPC's Regulatory Strategy 2022-2027.

The DPC was active in this space in 2023, producing four guides in relation to children's data protection rights under the GDPR which addressed various issues including the age of digital consent.

# Further insights on the DPC's 2023 Annual Report

## Children's data protection rights

Further, the Report details how, throughout 2023, the DPC engaged with educational bodies in the context of data protection practices in education settings. The DPC has commenced drafting a new "Data Protection Toolkit for Schools" which includes a detailed guidance document, a sample data protection impact assessment template, and tips on what to include in relevant school privacy policies.

Decisions and fines issued by the DPC in 2023 emphasise the high threshold to be met when processing children's personal data and protecting children's data protection rights. Data controllers must be able to clearly justify and document the processing of children's personal data, and where possible, incorporate proper data protection procedures and practices by design and default. The Report notes that transparency of processing and communication with data subjects is also key.

The DPC was also nominated as a representative member of the newly formed Task Force on Age Verification under the Digital Services Act and has engaged extensively with Coimisuin na Mean in relation to Ireland's first Online Safety Code, which is due to come into force later this year.

# Further insights on the DPC's 2023 Annual Report

## CCTV

One of the key focus areas for the DPC as highlighted in the Report is the deployment and use of surveillance technologies, particularly at large scale or in areas where there is a higher expectation of privacy (such as restrooms). The DPC published a revised version of its CCTV guidance to provide clarity to data organisations in this regard.

The Report details several cases involving the use of surveillance technologies such as CCTV systems, Advanced Number Plate Recognition technology and body-worn cameras.

The DPC stresses that where these technologies are used, the lawful basis for processing personal data must meet the standard of precision, clarity and foreseeability required under EU law. Several inquiries into local authorities during 2023 resulted in fines and temporary bans on the operation of CCTV cameras in certain locations. The decisions underline that organisations (including governmental entities and local authorities) must have a clear justification and lawful basis for the use of CCTV footage and other surveillance measures. CCTV must only be deployed when it is necessary and proportionate to do so.

A further case study contained in the Report involves the use of CCTV in a restaurant restroom, which was installed by an organisation for the purpose of preventing anti-social behaviour and other risks. The DPC noted that the data controller had not adequately demonstrated that the CCTV was necessary, as no strong evidence of previous incidents or issues was provided, nor evidence to suggest that CCTV would prevent anti-social behaviour and/or reduce the risk of slips, trips or falls.

# Further insights on the DPC's 2023 Annual Report

## CCTV

The DPC ordered that the restaurant switch off the cameras and securely delete all footage stored until a comprehensive assessment demonstrating justification for the CCTV was concluded.

This case reiterates the importance of not only completing risk assessments – the DPC requested a copy of the legitimate interest assessment – but supporting the conclusion of those risk assessments with strong documentary evidence.

During 2023, the DPC also consulted in relation to three draft codes of practice prepared under the Circular Economy and Miscellaneous Provisions Act 2022. The aim of the DPC was to ensure that the codes provided a clear legal basis for local authorities to use CCTV and other recording technologies where necessary, proportionate and in the public interest to do so. The three codes of practice were finalised by the end of 2023.

[The DPC's updated CCTV guidance can be found here. \(PDF, 525KB\)](#)

# Further insights on the DPC's 2023 Annual Report

## Final word

In the Report, noteworthy references are made to two separate topics, being reprimands and AI.

The DPC issued numerous reprimands in 2023. The DPC's power to issue reprimands was expanded by the addition to section 109 of the Data Protection Act 2018 allowing the DPC to issue reprimands outside of the inquiry process.

Organisations should note that while in certain cases the DPC may issue reprimands as the sole corrective measure, reprimands will form part of any consideration of potential future action by the DPC against a data controller.

Regarding developments in connection with AI, the DPC is taking a proactive approach. The DPC is engaging with tech companies and stakeholders to ensure data protection concerns are taken into account and incorporated into the design of AI software and products at an early stage.

We advise organisations to leverage their existing GDPR toolkits in preparation for complying with the GDPR as they roll out their AI programme.



# Empowering employees with AI chatbots

Date of issue: 18 September, 2024

# Empowering employees with AI chatbots

**Artificial Intelligence (AI) chatbots have gained prominence for their versatility and efficiency. To fully realise their benefits, employees need to be equipped to use these tools effectively while being aware of the potential risks.**

AI has become a cornerstone of modern business, revolutionising how companies interact with customers, manage processes, and make decisions. Chatbots are one of the many AI tools available, and they are widely used in customer service, human resources (HR), supply chain management, and as digital assistants in the workplace.

## AI chatbot applications

AI chatbots have transformed several sectors by automating routine tasks and boosting efficiency. For example, in customer service, they provide quick responses to inquiries, resolve issues, and anticipate needs, allowing human agents to focus on complex matters. In HR, chatbots streamline processes from recruitment to offboarding, freeing HR teams for more strategic work. In supply chain management, they track shipments, manage inventory, and predict demand through real-time data analysis.

Despite these advantages, integrating AI chatbots into business operations carries significant risks, including data privacy concerns, potential inaccuracies, and over-reliance on automation.

# Empowering employees with AI chatbots

## Risks of AI chatbots

A primary concern of AI chatbots is data privacy and security. For one, AI systems can become significant targets for cybercriminals. A recent report from the Dutch Data Protection Authority highlighted that personal data breaches occur when employees share personal data with chatbots, offering unauthorised access and opportunities for misuse.

Another significant risk is the possibility of providing inaccurate information. AI chatbots are only as good as the data and algorithms that power them. If not properly trained or updated, they can deliver incorrect or misleading information, potentially harming customer trust, leading to legal liabilities, or resulting in poor business decisions.

## Mitigating the Risks

To harness the power of AI chatbots while minimising associated risks, businesses can take proactive steps. Employee training is crucial. Staff should be educated on how to use AI chatbots correctly, understand their limitations, and know which types of information should not be shared with these tools. Regular training sessions will help ensure employees stay up to date with best practices and any changes to the chatbot's capabilities or protocols.

Updating the company's risk register to include AI-related risks is another important step. By systematically identifying, assessing, and monitoring these risks, companies can develop targeted strategies to address potential issues before they escalate.

Additionally, companies should complete or update their Data Protection Impact Assessment (DPIA) to cover the use of AI chatbots. This ensures that data privacy concerns are addressed and that appropriate safeguards are in place to protect sensitive information. The DPIA should also evaluate the chatbot's data handling practices, security measures, and compliance with relevant regulations.



# Empowering employees with AI chatbots

## AI governance, data protection, and HR considerations

Effective AI governance is essential for responsible AI usage. The new EU AI Act promotes establishing a framework that categorises AI systems by risk, distinguishing between high-risk systems and general-purpose AI. Businesses should implement and enforce relevant AI policies while ensuring that AI applications align with appropriate use cases.

From a data protection perspective, the interaction of AI with GDPR requires careful consideration. It is important that companies select the appropriate legal basis for processing personal data through AI chatbots. For customer-facing businesses, this often involves obtaining consent from customers before processing their data. Ensuring that consent is properly collected and documented is essential to meet regulatory requirements and maintain customer trust.

In HR, introducing clear policies on AI usage is vital. These policies should be reflected in employment contracts and regularly updated. Businesses should prevent "Shadow AI"—the unauthorised use of AI technologies by employees, which parallels "Shadow Tech" issues in data protection. This requires vigilance and clear communication to ensure AI is used appropriately within the company.

## Harnessing AI

AI chatbots offer transformative benefits across various business functions, but their successful implementation requires a strategic approach. Employees should be well-trained to maximise these tools while mitigating risks related to unauthorised use of information, data breaches, misinformation, and over-reliance on automation.

By prioritising robust AI governance, data protection practices, and clear HR policies, companies can fully harness AI chatbots to enhance productivity, improve efficiency, and maintain stakeholder trust.

# Navigating Legitimate Interests Assessments

Date of issue: 14 October, 2024

# Navigating Legitimate Interests Assessments

This month, the CJEU confirmed that a solely commercial interest can qualify as a legitimate interest under the GDPR. This decision provides certainty for organisations which rely on legitimate interests as a legal basis for processing personal data, but it is important that Data Controllers continue to assess, on a case-by-case basis whether the intended processing could be accomplished in a less intrusive way for the impacted individuals.

## Understanding Legitimate Interests

Legitimate interests is one of the six lawful bases for processing personal data under the GDPR. One of the key requirements to be able to rely on legitimate interests as a legal basis is to demonstrate that the processing is justified and proportionate.

Our recommendation is to ensure a thorough Legitimate Interests Assessment (LIA) is documented, detailing each step of the process and outlining the conclusions reached. This documentation serves as evidence for the regulatory authorities and also demonstrates that the organisation complies with the accountability principle.

Once the LIA is completed, organisations must understand that it is not a one-off exercise, LIAs should be periodically reviewed and updated to reflect any changes in processing activities or regulatory requirements.

# Navigating Legitimate Interests Assessments

## Step-by-step guide to conducting a Legitimate Interests Assessment contd.

### 1. Identify the purpose

The first step in an LIA is to clearly define the purpose of the data processing. Organisations must articulate why the processing is necessary and how it aligns with their legitimate interests. This could include activities such as training AI models, direct marketing, or transferring customer data within the same company group.

### 2. Assess necessity

Once the purpose is identified, the next step is to evaluate whether the processing is necessary to achieve that purpose. As outlined above, organisations should consider if there are less intrusive means to achieve the same result when the purpose is purely commercial. This assessment will help ensure that the data processing is proportionate and justified.

### 3. Balance the interests

The core of the LIA is the balancing test, where organisations weigh their legitimate interests against the potential impact on individuals' rights and freedoms. This involves considering factors such as the nature of the data, the context of the processing, and the reasonable expectations of the data subjects. Organisations should document their findings and rationale to demonstrate compliance. The DPO is a key figure in this part of the assessment.

### 4. Implement safeguards

If there are risks identified as part of the assessment, organisations should implement appropriate safeguards in order to mitigate them, where possible. These might include data minimisation, anonymisation, or enhanced security measures. Ensuring transparency with data subjects about the processing activities and their rights is also crucial.

### 5. Governance

The DPO must oversee the LIA process, ensuring compliance with data protection requirements and providing guidance when needed. It is recommended to involve Business Unit Leaders to support on the completion of the balancing test by providing insights into the business rationale for data processing.

# Navigating Legitimate Interests Assessments

## Key elements of a Legitimate Interests Assessment

As a summary, a comprehensive LIA should include the following key elements:

### Purpose Description

- A clear and detailed explanation of the purpose of data processing.

### Necessity Test

- An assessment of whether the processing is necessary for the stated purpose.

### Balancing Test

- A detailed analysis weighing the organisation's interests against the potential impact on individuals.

### Risk Mitigation Measures

- A description of the safeguards implemented to protect data subjects' rights.

### Documentation

- Thorough records of the LIA process, including the rationale for decisions made and the involvement of key parties such as the DPO or any other relevant members of the Privacy Team.

### Review Mechanism

- A plan for regular reviews and updates to the LIA to ensure ongoing compliance.

# International Data Transfers

Date of issue: 25 January, 2024

# International Data Transfers

A look back on 2023 and what to expect for 2024.

A stated aim of the GDPR is the free flow of personal data between Member States.

The transfer of personal data to countries outside the EEA however requires special consideration.

In essence, in Europe you cannot send individuals' personal data outside of the EEA – it's prohibited, unless you can satisfy one of the exceptions to this general rule.

Transfers outside the EEA require:

- (i) An adequacy decision to be in place in the country the personal data is being transferred to; or
- (ii) Appropriate safeguards must be in place to secure the transfer of personal data; or
- (iii) Reliance on a derogation, as set out in the GDPR.

Trust is key when it comes to data transfers internationally. Remember that privacy and data protection are fundamental rights, which stem from human rights, and therefore the rights of EU data subjects should flow where their data goes.

Organisations must map where personal data goes, and if it leaves the EEA, then your organisation must illustrate where the personal data travels to and ensure that the correct transfer mechanism is in place to safeguard the individuals' rights.



## Let's talk a little bit more about adequacy

Adequacy decisions are formal decisions made by the EU which recognise that another country, or territory provides an equivalent level of protection for personal data as the EU.

These decisions are based on an investigation on the part of the European Commission ("the Commission"). The Commission will consider the rule of law, respect for human rights, local legislation, access of public authorities to personal data and many other such investigations. Once a country is granted adequacy, it is subject to review every 4 years.



## What is the situation with transfers of personal data to the USA?

The past few years have seen some turbulence with transferring personal data to the USA.

The Data Privacy Framework (the "DPF") is now in place, and the question on everyone's mind is whether we can expect a challenge to the DPF in 2024? While it is possible, there is optimism that the DPF has adequately addressed the concerns raised in the decisions that lead to the striking down of Safe Harbour and the Privacy Shield.

It's also a positive step that the USA implemented changes to its national security laws to better align with the EU requirements for surveillance on the processing of EU citizens' personal data. The view for now is that the DPF is a stable mechanism for transfers while taking into account the concerns of the CJEU in the Schrems II ruling.

# International Data Transfers

A look back on 2023 and what to expect for 2024.

## What are the appropriate safeguards?

If there is no adequacy decision, then 'appropriate safeguards' may be used to legally transfer personal data internationally.

Appropriate safeguards are legal tools designed to ensure recipients of personal data outside the EEA process and protect personal data to the same standard as Europe. All the safeguards require prior approval from a supervisory authority.

Helpfully the GDPR sets out a list of appropriate safeguards that a data controller or data processor may rely on. We set out below details for two of the appropriate safeguards:

1. Binding Corporate Rules (BCRs) allow a large multinational company to adopt a policy suite with rules for handling personal data that are binding on the company. Once a competent supervisory authority signs off on the rules, then the company is free to transfer personal data around the world within their organisation.
2. Standard Contractual Clauses (SCCs) are model data transfer terms expressly approved by the European Commission, which are non-negotiable, and which are designed to help controllers and processors transfer personal data outside the EEA lawfully. In our experience, SCCs are the most commonly used appropriate safeguard.

As mentioned at the outset, there is the option to rely on a derogation or a restriction when it comes to the transfer of personal data internationally. However, these transfer mechanisms are seen as a last resort where there is no adequacy decision and there are no appropriate safeguards in place.



## Predictions for this year

We will see a review of the DPF; which will be interesting to keep an eye on to see how it is settling in and working in practice.

We have already seen a review of 11 adequacy decisions which were decided pre-GDPR, you can read our analysis [here](#). We will potentially have a new adequacy decision for Brazil, depending on how the talks progress

There is lots to watch out for in the sphere of international data transfers. Stay in touch with us as we continue to highlight any changes in this area.



To learn more about our insights on recent developments on international data transfers, as well as to what to expect for the year ahead you can watch our [Think Law Series](#)



# The 5 Most Common Data Privacy Mistakes of 2023 (and How to Prevent Them)

Date of issue: 2 January, 2024

# The 5 Most Common Data Privacy Mistakes of 2023 (and How to Prevent Them)

For most organisations, data privacy is considered a “top-10” organisational risk. We know that keeping up with all data privacy requirements can be challenging. We’re here to help. Here are some of the most common data privacy mistakes made in 2023, and how to avoid them.

## 1 Mistake: Selection and application of an inappropriate legal basis

During 2023, the DPC issued several fines to organisations who relied on a legal basis that was not suitable for the data processing undertaken.

Some organisations fail to carry out the “necessity test” to ensure that the personal data processed is necessary to carry out a specific activity before relying upon a legal basis such as performance of a contract or legitimate interest.

**How to prevent it:** Organisations must carefully assess the purpose of their data processing to identify the legal basis that is most appropriate. When relying on a specific legal basis, it is recommended to document the reasons and, in the case of relying on legitimate interest a legitimate interest assessment must be undertaken.

## 2 Mistake: Failure to maintain appropriate Record of Processing Activities (“RoPA”)

Under the GDPR, organisations are obliged to maintain a RoPA. When the Data Protection Commission (DPC), conducted a review of organisations’ data protection records, it found many of these records were insufficient and non-compliant. This exposed the organisations in question to penalties under the GDPR.

**How to prevent it:** Organisations must conduct a data mapping exercise with input from several business functions, to identify exactly what data is held and where. Every business function should be broken down and the RoPA should be as detailed as possible. It is expected that organisations have their RoPA ‘ready to go’ at any time, and in any event, within 10 days’ notice of a request from the DPC.

## 3 Mistake: Not prioritising training

Privacy training is one of the key factors to ensure all employees in an organisation understand their obligations under the GDPR and any other applicable privacy regulations (the “data protection rules”). A lack of training increases the risk of human error when employees are dealing with personal data (e.g., failure to safeguard personal data, or sharing data with unauthorised persons). This can lead to breaches and potentially fines and reputational damage.

**How to prevent it:** Training should be tailored to the different roles and responsibilities of each employee to ensure it is relevant and in line with the processing activity. It should also be an ongoing activity to guarantee that all employees, including new joiners and contractors, understand the importance of processing personal data in a compliant manner.

# The 5 Most Common Data Privacy Mistakes of 2023 (and How to Prevent Them)

4

## Mistake: Believing in a one size fits all approach

There's a tendency to think that using generic privacy templates will ensure compliance with the requirements laid out in the data protection rules. However, this practice presents a risk as each organisation and its business units will process personal data for different purposes and will require the implementation of different technical and organisational measures. Following a one size fits all approach exposes an organisation to sanctions or penalties under the GDPR for failing to comply with the principles of data protection by design and default.

**How to prevent it:** Following the data protection by design and by default requirements is crucial to ensure that your organisation tailors its privacy framework to its specific processing operations. Your organisation should assess the inherent characteristics, size, range, and circumstances of the processing as well as the purpose to implement the appropriate technical and organisational measures and safeguards.

5

## Mistake: Believing compliance with one regulation equals compliance with all privacy regulations

The data protection rules are constantly evolving, and new laws and regulations are orbiting the data protection and privacy compliance landscape. When implemented in May 2018, the GDPR marked the beginning of global privacy regulations. However, the GDPR isn't the only player in the game anymore, and organisations must consider what other privacy regulations apply to them based on the nature of their business and locations. Other legislative texts like the Digital Service Act, the e-Privacy Directive, the AI Act or national data protection acts operating in the locations where your organisation is based might impact your privacy framework.

**How to prevent it:** It is key to understand the organisational structure of the company, assess the locations where the organisation is based and whether those locations have specific privacy laws in place.



## How can KPMG help?

Our team can help you identify any gaps in your privacy programme, design and deliver a data protection framework, and complete an assessment of all the different privacy laws that will be applicable to your organisation and how to comply with them.

# Refresher on Legal Basis

Date of issue: 5 December, 2023

# Refresher on Legal Basis

As the year draws to a close and we reflect on recent data protection updates, guidance and decisions, our team has prepared a refresher on the legal grounds for processing of personal data, and what you need to consider when relying on a particular legal basis.

Accountability is one of the key principles which underpins the GDPR. When considering which legal basis your organisation relies upon for processing personal data, we recommend you back up your decision with an objective justification.

Let's now illustrate how each legal ground can be relied upon.

## Consent

- The Data Subject must give consent freely and unambiguously.
- Consent must be presented in clear and plain language so that it is informed.
- Data Subject must be able to withdraw consent.

## Performance of a Contract

- Processing must be necessary to deliver the contractual service.
- If the contract is with a child, the organisation needs to ensure the child has the necessary competence to enter the contract.

## Legal Obligation

- Your organisation must be obliged to process the personal data to comply with an EU or national legislation or the common law.
- The processing operations must be necessary to comply with the legal obligation.
- The law should make clear the purposes of the processing and must meet an objective of public interest.

## Vital Interests

- Processing of personal data is needed to protect someone's life or mitigate against a serious threat to a person (e.g., in a medical or healthcare situation).
- This legal basis is less likely to be appropriate for large scale processing.


# Refresher on Legal Basis

## Public Task

- Appropriate where your organisation is a Public Authority or exercises official authority or carries tasks of public interest (e.g., professional associations)
- The processing under this legal basis should be grounded on EU or national law

## Legitimate Interest

- Your organisation should consider the three elements needed for this legal basis:
  1. The **purpose** test. Identifying a legitimate interest which they or a third party pursue.
  2. The **necessity** test. Demonstrating that the intended processing of the data subject's personal data is necessary to achieve the legitimate interest.
  3. The **balancing** test. Balancing the legitimate interest against the data subject's interests, rights, and freedoms by carrying out a Legitimate Interest Assessment.

 Data controllers must consider how their data processing activities fit within the above grounds. It is worth bearing in mind that the lawful bases as set out in Article 6 are not hierarchical, and each of the six grounds rank equally and can be validly relied upon. The facts of each processing activity will determine the most appropriate legal basis for processing personal data.

Finally, in line with the principle of data minimisation, processing of personal data should only be undertaken in a limited way, where relevant and necessary to achieving the purpose of the processing. To ensure accountability, controllers should record their reasoning as to why they thought it necessary to process personal data under the different legal basis as outlined above.

## How can we help?

Our team can support you by:

- Ensuring that the legal basis chosen for the processing of data is the appropriate one.
- Carrying out a Legitimate Interest Assessment.
- Ensuring your consent management practices are compliant with the GDPR.
- Reviewing the privacy policies and contracts with the data subjects to ensure they meet the transparency obligations.

**Black Friday is Almost Here.**

**Is Your Marketing Campaign Compliant?**

# Black Friday is Almost Here. Is Your Marketing Campaign Compliant?

*For many retailers in Ireland and across the globe, Black Friday and Cyber Monday are the most important shopping days of the year. In this article, we look at how to make sure your Black Friday marketing campaign is compliant with the law.*

## Am I engaging in Direct Marketing?

Direct marketing involves targeted communications to an individual, where a product or service is being promoted. This includes messages to promote events, ideals or organisations, or to get potential customers to request additional information about a product or service.

Further, if a communication has multiple purposes, and just one of those purposes is the promotion of a product or service, it will be categorised as a direct marketing communication.

If your Black Friday marketing campaign involves sending promotional emails, texts, or other targeted advertisements to individuals, then you are engaging in direct marketing and you need to make sure you're compliant with the law.

**A key driver of sales is successful targeted marketing campaigns, but there are legal consequences to getting a marketing campaign wrong, which is why it is vital that direct marketing communications are compliant with the law.**

## How can I ensure compliance?

In Ireland, direct marketing is governed by the GDPR, the Data Protection Act 2018 and the ePrivacy Regulations.

As a general rule, in order to ensure compliance with the law, specific and informed consent should always be obtained from an individual prior to sending any form of direct marketing communications. The GDPR makes it clear that silence, pre-ticked boxes, or inactivity on the part of a data subject will not amount to valid consent. There may be circumstances where a soft opt-in can be relied upon as a basis for direct marketing under the ePrivacy Regulations, provided certain conditions are met.

Further, it is important to make sure that data subjects are made aware of their right to withdraw their consent at any time. To facilitate this an "opt-out" must be included with each marketing communication.

We also recommend you review your marketing lists to ensure they are up to date and that any customer who has opted out of receiving marketing communications is removed from the database and does not receive any communications.



# Black Friday is Almost Here. Is Your Marketing Campaign Compliant?

*In this article, we look at how to make sure your Black Friday marketing campaign is compliant with the law.*

## **We're here to help**

With Black Friday and the Christmas season approaching, retailers need to ensure compliance with direct marketing rules in order to avoid data subject complaints, potential data protection fines, or negative publicity. We recommend that all relevant businesses / organisations take steps to familiarise themselves with best practices when it comes to direct marketing.

For more information regarding direct marketing and data protection concerns, including how it might be possible to rely on the lawful basis of legitimate interests for a marketing campaign, a marketing soft opt-in, or how to differentiate between a marketing message and a service message, contact a member of our data protection team.



# Contact us



**Emma Ritchie**

Head of Data Protection & Privacy

e: [emma.ritchie@kpmglaw.ie](mailto:emma.ritchie@kpmglaw.ie)

Tlf: +353 87 050 4628



[kpmglaw.ie](http://kpmglaw.ie)