JOIC
JERSEY OFFICE OF THE
INFORMATION COMMISSIONER

Data Protection Maturity Survey 2026

March 2026

Introduction

As part of the commitment to upholding the highest standards of data protection, the Jersey Office of the Information Commissioner (JOIC), in collaboration with the Isle of Man Information Commissioner (IoM IC), conducted a Data Protection Maturity Survey with the support of registered organisations across the two jurisdictions.

This coordinated initiative was designed to understand how organisations are implementing the principles of their respective data protection laws.

The survey examined key areas of data protection activity, including data protection training, data protection roles and responsibilities, responding to data subject rights requests and the adoption of emerging technologies.

This report presents the findings for organisations registered with the Jersey Office of the Information Commissioner.

The conclusions are being used to:

- Understand current levels of compliance and good practice
- Identify areas for improvement
- Inform the future design of tailored guidance and support where needed
- Strengthen the overall data protection culture across each island
- Support the delivery of our strategic priorities

The survey was undertaken in line with the Market Research Society Code of Conduct which guides all those engaged in research, insight and data analytics in maintaining professional standards. Regard was also paid to the Code of Practice for Tier 1 Statistics (the guidelines for public authority statistics producers in Jersey).

All figures in this report have been rounded independently. As a result, figures presented in tables and charts may not equal the sum of their component values.

Methodology

SAMPLE

All organisations registered with the Data Protection Authority and the Isle of Man were invited to participate. This report details Jersey responses only.

SURVEY DESIGN

An online survey was sent to Data Protection Officers and Data Protection Leads

WEIGHTING

Survey data has been cleansed & weighted by organisation size (FTEs) and primary industry

Survey Respondents

439 of Jersey-registered organisations responded to the survey

Because of sampling, reported percentages are subject to a margin of error of ±4.57 percentage points.

For analysis, organisations have been grouped by size and primary industry to enable meaningful comparisons:

- 0–9 FTE (small)
- 10–50 FTE (medium)
- More than 50 FTE (large)

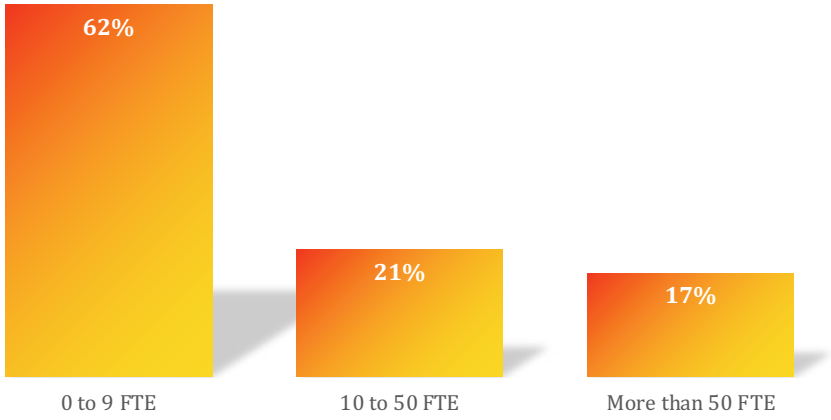
Differences by organisation size or industry are reported only where there is **statistical evidence** that they represent true population differences rather than sampling variation.

A total of 439 organisations responded to the survey from a population of approximately 8,000 registered organisations. This level of participation provides a sufficient sample size to support robust analysis at the overall level. While the response rate of 5.4% may appear low, it falls within expectations for voluntary external business surveys, particularly when conducted online and without mandatory participation.

As with all surveys, the results are subject to a degree of statistical uncertainty. At the overall level, percentages are subject to a margin of error of approximately ±4.6 percentage points. This means that small differences should be interpreted with some caution, while broader patterns and larger differences are likely to reflect genuine differences across the population.

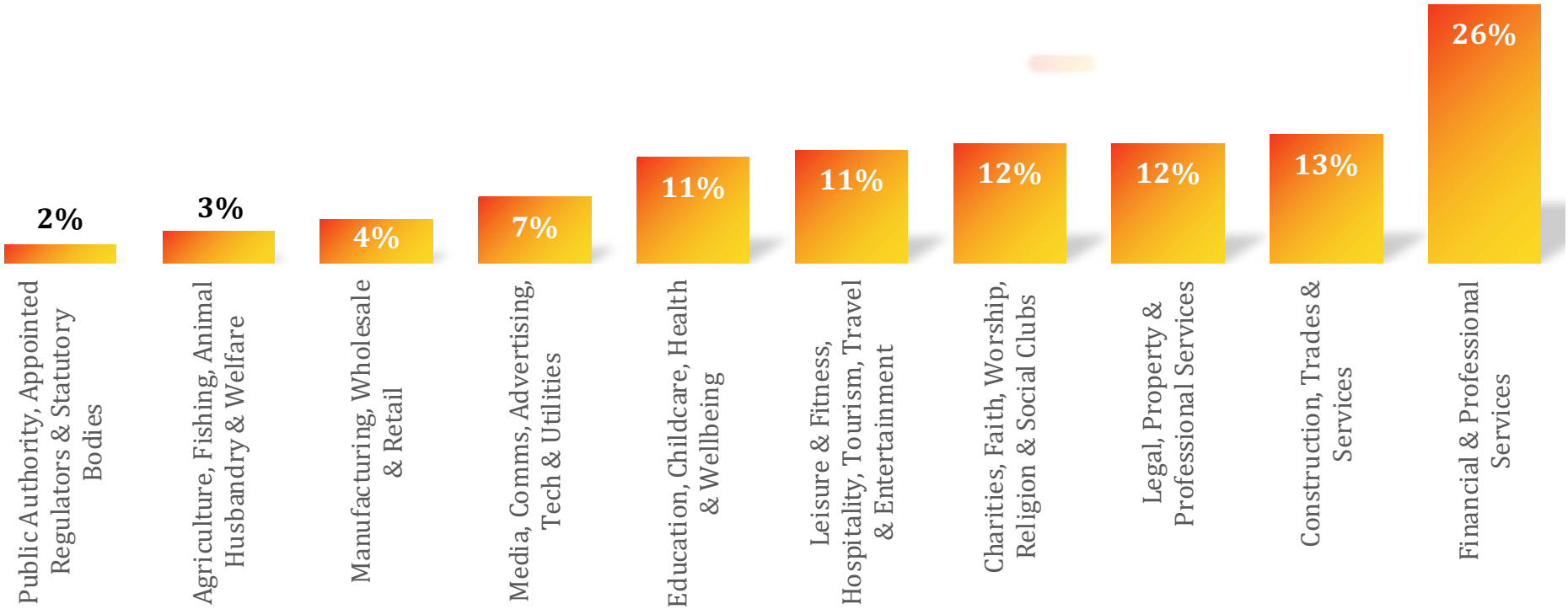
The findings therefore provide a reliable overview of data protection practices at the aggregate level.

Survey respondents by organisation size (FTE)



Survey Respondents

Survey respondents by primary industry



Executive Summary

- Data protection maturity is closely associated with organisational size and regulatory context. Larger organisations and those operating in the Finance and the Public Sectors generally demonstrate more structured and embedded governance arrangements.
- 70% of organisations with 10 or more FTE provide data protection training to staff. Role-specific training is less widely adopted. Most small organisations report confidence in their understanding of data protection responsibilities however uptake of formal training remains limited.
- 44% of organisations have appointed a DPO and a further 39% have designated a Data Protection Lead, but formal assessment of professional expertise prior to appointment is uncommon. Many DPOs and Data Protection Leads also hold operational roles involving decision-making about personal data.
- Almost half of organisations report no current use of AI. Where AI is used, activity is largely focused on document drafting and marketing or research functions.
- Awareness of data protection risks associated with AI tools is high among registered organisations.
- 2/3rds of organisations have never conducted a DPIA or DPIA-style assessment, and uncertainty remains about when such risk assessments are legally required.
- 2/5ths of organisations record all personal data breaches, a significant proportion report keeping no formal record of incidents.
- 2/5ths of organisations also report having no formal cyber-security policies and procedures in place.

JOIC Strategic Priorities 2026 – 2028

The Data Protection Maturity Survey results provide essential baseline quantitative data set to help us measure progress.

JOIC will deliver the three strategic priorities combined with a more proactive approach to enforcement and then remeasure in 2-years.

The results of the survey will help to inform JOIC's services and programmes.

JOIC Strategic Priorities 2026 – 2028

Children's Privacy

To foster a safer digital environment to ensure that children's personal data is safeguarded by setting clear standards for organisations, promoting responsible design of digital services, and taking strong enforcement action where risks to children are identified.

Artificial Intelligence

Promote responsible local use, development and deployment of AI-driven technologies by ensuring compliance with data protection laws and principles, thereby safeguarding individuals' rights, fostering innovation, and establishing a trusted framework for ethical AI use.

Cyber Security

Strengthen organisations' data security and cybersecurity protections to reduce the risk of data breaches, enhance resilience against cyber threats, and ensure the ongoing privacy and safety of individuals' personal data.

We will be taking a three phased approach of Advise, Assess and Act, to deliver the strategic priorities. This approach to their delivery is transformational.

Advise is the phase where we support individuals and organisations to improve their data protection practices by providing information, guidance, and rights support.

Assess being the phase which focuses on gathering intelligence and evaluating how well data is being protected. Its purpose is to build an evidence base, identify high-risk practices, and understand where intervention is most needed.

Finally, where necessary, we will **Act** initiating regulatory action to address breaches and enforce the law. This phase addresses non-compliance and drives accountability. Its purpose is to deter misconduct, protect the public from harm and reinforce that standards are mandatory not optional.

Data Protection Training and Knowledge

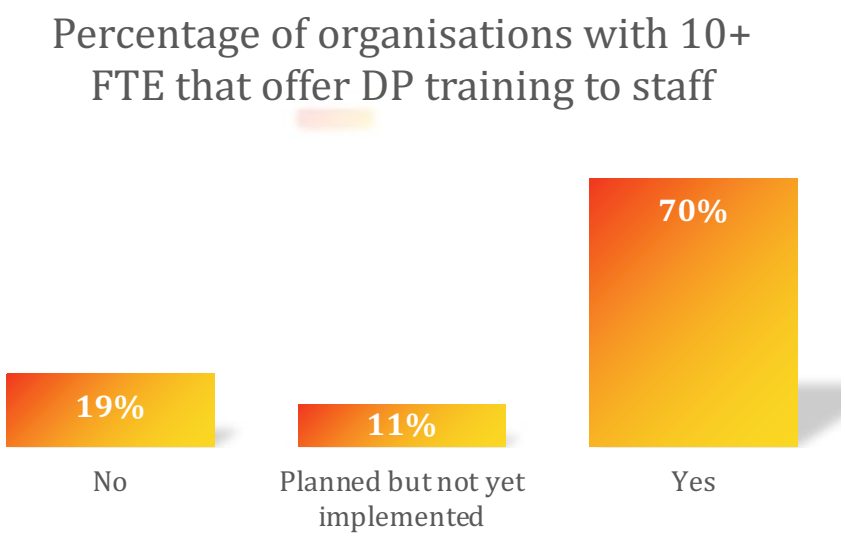
Data Protection Training in Medium-Large Organisations

70% of organisations with **10 or more FTE** provide data protection training to staff.

Induction (**88%**) and periodic refresher training (**81%**) are the most common forms of training on offer.

Role-specific training is not widely adopted (**38%**).

Half (**50%**) deliver training through 'in person' or 'classroom' style sessions, while **54%** offer pre-recorded or self-paced online modules.



38% of larger organisations say '**Lack of time and operational pressures**' are the greatest barrier to offering staff data protection training

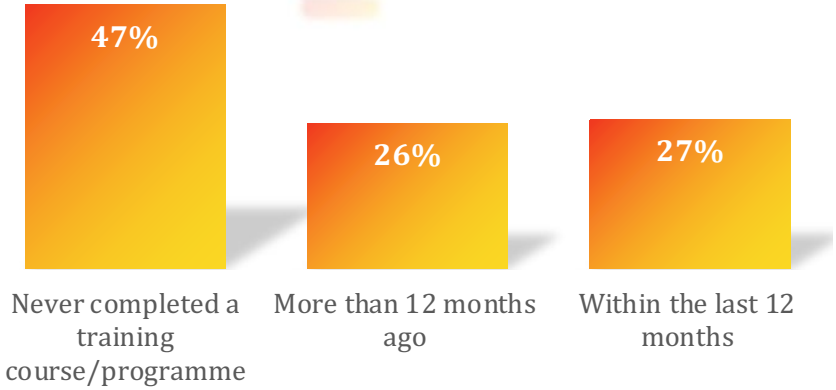
Data Protection Knowledge in Small Organisations

Among smaller organisations (**with fewer than 10 FTE**), around half (**52%**) take regular steps to keep their data protection knowledge up to date.

Reading online articles or guidance is the most common method of staying informed on data protection obligations (**68%**).

While two-thirds (**65%**) feel confident in their understanding of data protection responsibilities, almost half (**47%**) have never completed a formal training course.

Percentage of small organisations (0 to 9 FTE) that have completed a formal training course



88% of small organisations say they are aware that they can contact JOIC for advice and guidance if needed

Key Differences by Primary Industry

Data Protection Training

	Organisations that have appointed a DPO	Organisations that protect their DPOs independence in policy and practice
Agriculture, Fishing, Animal Husbandry & Welfare	70%	29%
Charities, Faith, Worship & Religion & Social Clubs	58%	56%
Construction, Trades & Services	13%	25%
Education, Childcare, Health & Wellbeing	77%	67%
Financial & Professional Services	96%	77%
Legal, Property & Professional Services	81%	44%
Leisure & Fitness, Hospitality, Tourism, Travel & Entertainment	77%	47%
Manufacturing, Wholesale & Retail	54%	20%
Media, Comms, Advertising, Tech, Utilities & Delivery Services	86%	39%
Public Authorities, Regulators & Statutory Bodies	100%	100%

JOIC Comment – DP Training

- Training is the consistent matter raised in all enforcement actions - ‘Lessons Learned’ – current levels of data protection training are insufficient to support the DP demands faced by organisations.
- Smaller organisations with fewer than 10 employees need effective data protection training which is affordable, practical, Jersey-centric and time efficient.
- The lack of role-specific training is impacting fulfilling individual rights in a wholesome manner.
- Lack of data protection training is unacceptable and is no defence when we undertake Investigations or Inquiries.

JOIC Commitment – DP Training

- JOIC will refresh the DP training checklist to help organisations to select a training provider.
- JOIC will publish lessons learned to highlight where training needs to be reviewed or amended.

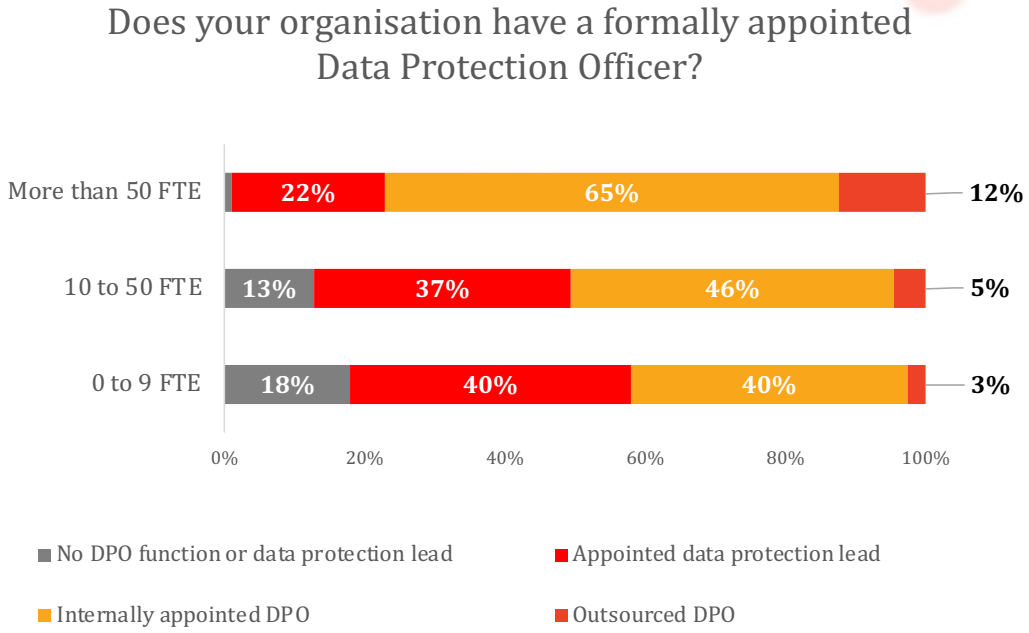
Data Protection Roles and Responsibilites

Data Protection Officer (DPO)

Around two-fifths (**44%**) of organisations have an appointed a Data Protection Officer (DPO), while a further two-fifths **39%** have designated an individual to lead on data protection matters.

Among those with a DPO, **90%** made the appointment without conducting a formal assessment of their professional qualities and expertise, although **42%** say there was some informal consideration.

Over half (**57%**) report that their DPO's independence is protected in both policy and practice.



Half (**49%**) of organisations say their DPO also holds a senior or operational role which involves making decisions about personal data

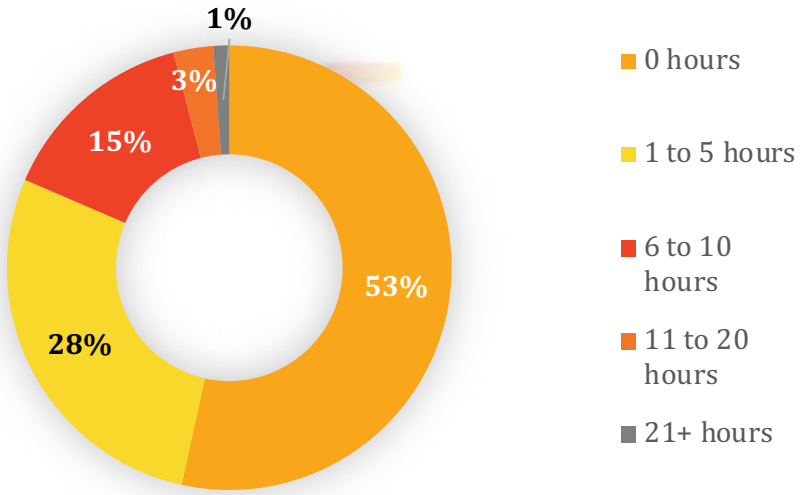
Data Protection Lead

Only **3%** of organisations with a Data Protection Lead appointed the individual following a formal assessment of their professional qualities and expertise.

Half (**53%**) report their Data Protection Lead had no structured data protection training in the past 12 months.

The majority (**57%**) of Data Protection Leads also hold a senior or operational role that involves decision-making about personal data.

Number of hours of structured training undertaken by the Data Protection Lead in the last 12 months



72% of organisations report that data protection matters are considered at board level, either as a standing agenda item (**37%**) or on an occasional basis a (**35%**)

Key Differences by Primary Industry

Appointing a DPO and Protecting Their Independence

	Organisations (10+ FTE) that offer DP training to staff	Organisations (0 to 9 FTE) that have undertaken a formal DP training course
Agriculture, Fishing, Animal Husbandry & Welfare	33%	22%
Charities, Faith, Worship & Religion & Social Clubs	54%	52%
Construction, Trades & Services	24%	24%
Education, Childcare, Health & Wellbeing	47%	29%
Financial & Professional Services	50%	84%
Legal, Property & Professional Services	51%	51%
Leisure & Fitness, Hospitality, Tourism, Travel & Entertainment	27%	50%
Manufacturing, Wholesale & Retail	34%	6%
Media, Comms, Advertising, Tech, Utilities & Delivery Services	30%	62%
Public Authorities, Regulators & Statutory Bodies	88%	86%

JOIC Comment - DPOs & DP Leads

- The role of DPO comes with significant statutory responsibilities which cannot be underestimated or diminished.
- Registered organisations must recognise the significance of this role.
- Respondents highlight a conflict in roles and lack of DP expertise in their appointed DPOs.
- DP leads appear to have little or no structured training in the preceding year.
- Welcome the statistic regarding board level DP discussions.
- We consider a DPO with insufficient expertise, knowledge and independence as an aggravating factor when undertaking an Investigation or Inquiry.
- Similarly, we consider a DP Lead exposed in DP matters due to lack of training, support or knowledge as an aggravating factor when undertaking an Investigation or Inquiry.

JOIC Commitment - DPOs & DP Leads

- JOIC will strive to engage with all DPOs and DP Leads to involve them in our Let's Go DPO events and newsletters.
- JOIC will refresh the DP training checklist to help organisations to select a training provider.
- JOIC will continue to update guidance on the role of the DPO.

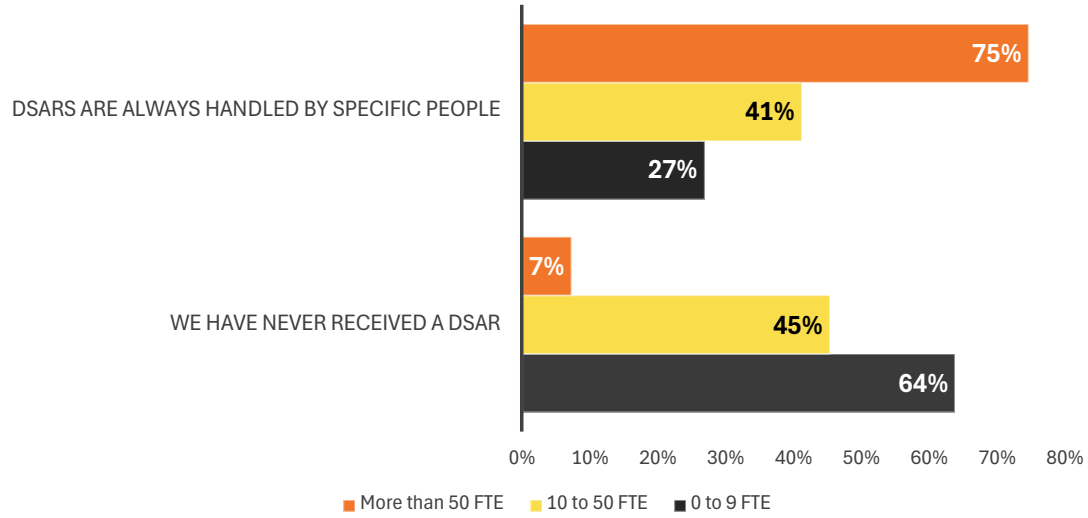
Data Subject Access Requests

Data Subject Access Requests (DSARs)

59% of organisations have never received a data subject access request (DSAR), although this is uncommon in larger organisations.

When DSARs are received, they are normally handled by the DPO or data protection lead (**55%**) or other employees (**28%**).

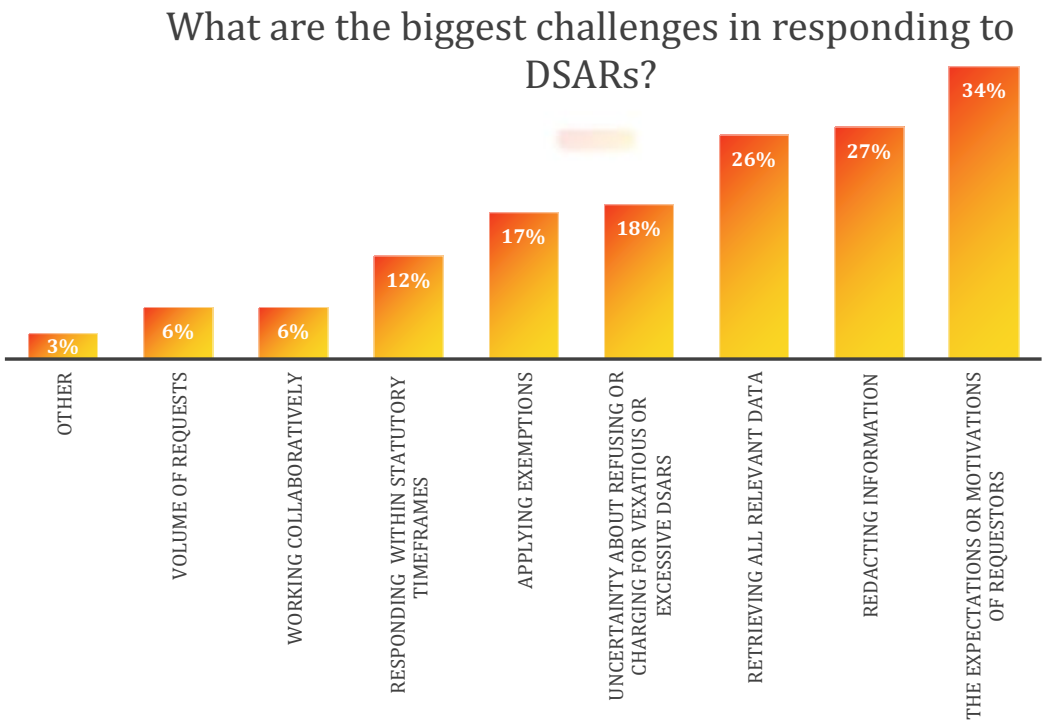
In larger organisations, DSARs are typically managed consistently by the same people.



Data Subject Access Requests

Half (**53%**) of all organisations provide dedicated DSAR training for those employees responsible for handling them.

Two thirds (**68%**) of organisations are confident in redacting information appropriately, however redaction remains one of the biggest challenges in responding to DSARs



JOIC Comment - Data Subject Access Requests

With 28% of organisations having DSARs handled by non DPOs or DP Leads – training is essential to ensure wholesome responses as per the Data Protection (Jersey) Law 2018.

The challenges in responding to DSARs further highlights where additional training is needed; redaction, understanding exemptions, scope of search parameters.

Welcome the 53% of organisations who are providing dedicated DSAR training for those employees responsible for handling them.

27% of organisations with fewer than 10 employees have received a subject access request. This sector reported the least training which exposes them to the risk of compliance issues.

JOIC Commitment - Data Subject Access Requests

JOIC will continue to offer awareness sessions on this topic.

JOIC will monitor and update our guidance on this topic where and when necessary.

JOIC will communicate with all registered organisations to invite them to join our newsletter subscription list for frequent updates.

Lack of training or understanding of individual rights is unacceptable and is no defence when we undertake Investigations or Inquiries.

Emerging Technologies

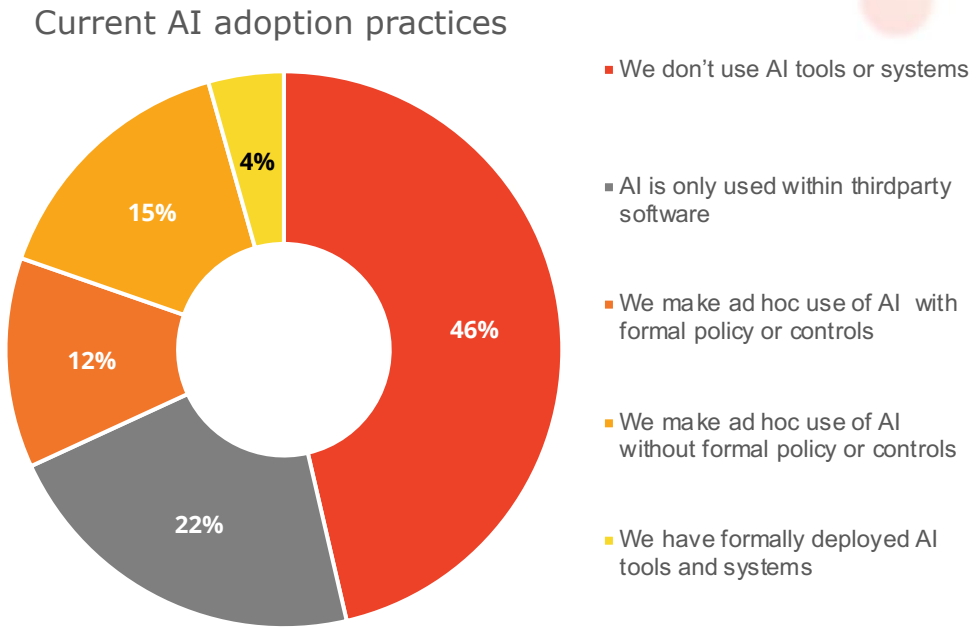
Adoption of Artificial Intelligence (AI)

Almost half of organisations (**46%**) report that they **do not currently use AI tools or systems.**

This ranges from **10%** of large organisations (50+ FTE) to **50%** of small organisations (0–9 FTE).

4% of organisations say they have formally deployed AI, while a further **12%** report ad-hoc use with policies and controls.

Among organisations using AI, around half (**48%**) use generative tools such as ChatGPT, and **14%** use speech or text recognition technologies.



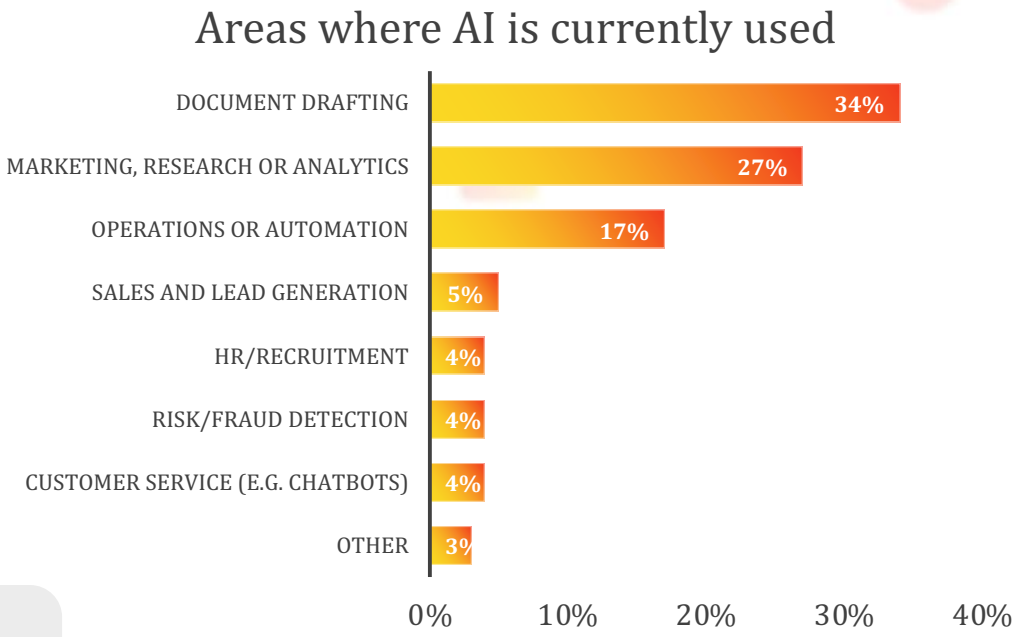
Only **10%** of organisations report processing personal data as part of their AI use

Risks with AI Tools and Systems

Organisations primarily use AI for document drafting (**34%**) and for marketing and research activities (**27%**).

Almost half (**47%**) report conducting a Data Protection Impact Assessment (**DPIA**) before implementing AI tools or systems.

Overall, **71%** say they have identified data protection risks associated with AI use, with half (**53%**) formally documenting these risks and **18%** addressing them through informal discussion.



The most frequently identified data protection risk was inaccurate or unreliable outputs impacting individuals

Key Differences by Primary Industry

AI Adoption and Use of DPIA Style Risk Assessments

	Organisations that have formally adopted AI or make ad-hoc use with controls	Organisations that have never conducted a DPIA style assessment
Agriculture, Fishing, Animal Husbandry & Welfare	2%	80%
Charities, Faith, Worship & Religion & Social Clubs	8%	86%
Construction, Trades & Services	9%	93%
Education, Childcare, Health & Wellbeing	8%	76%
Financial & Professional Services	24%	41%
Legal, Property & Professional Services	19%	69%
Leisure & Fitness, Hospitality, Tourism, Travel & Entertainment	14%	70%
Manufacturing, Wholesale & Retail	1%	79%
Media, Comms, Advertising, Tech, Utilities & Delivery Services	18%	83%
Public Authorities, Regulators & Statutory Bodies	63%	29%

JOIC Comment – Emerging Technologies

- The supply chain risks are seemingly being underestimated with 22% of respondents noting that ‘AI is only used within third party software’
- 15% of respondents are using AI without formal policies or controls.
- Welcome the 71% of respondents who report they have identified data protection risks associated with AI use.

JOIC Commitment – Emerging Technologies

- JOIC offers updated guidance on conducting a DPIA to help risk manage the implementation of AI
- JOIC provide Let's Go DPO bespoke AI implementation events – initially focussing on AI in HR
- JOIC will publish AI guidance and simple checklist
- The adoption of AI and the implications/risks on personal information will be carefully evaluated should a DP matter be investigated or an Inquiry undertaken.

Managing Data Protection Risks

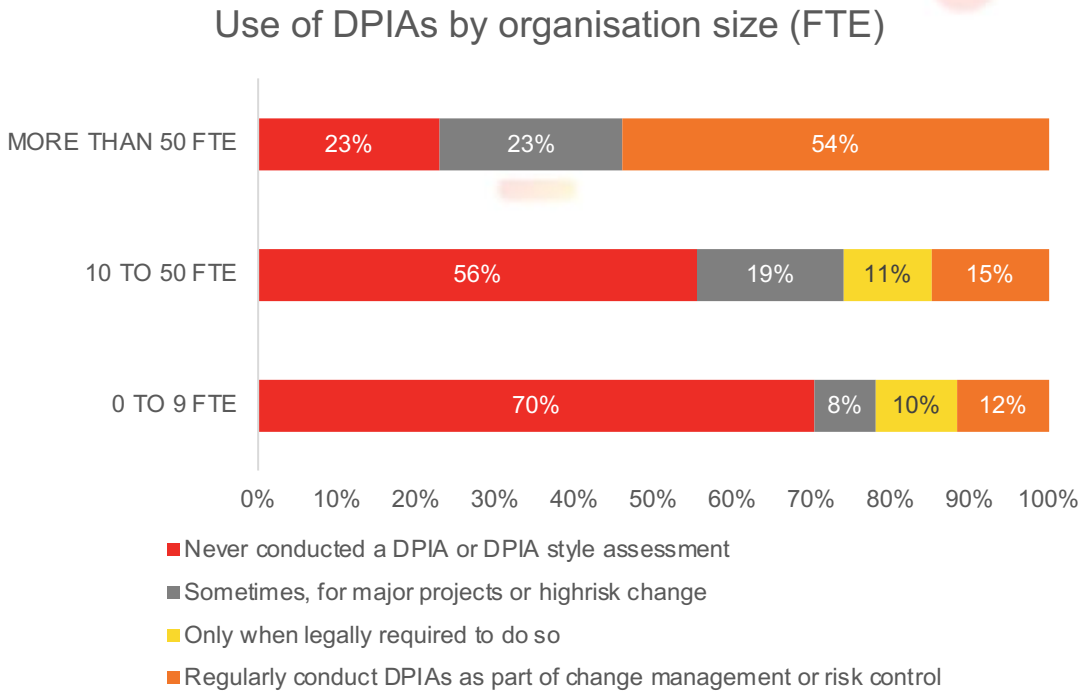
Data Protection Impact Assessments

Two-thirds of organisations (**67%**) report that they have never conducted a Data Protection Impact Assessment (DPIA) or a DPIA-style assessment.

While **41%** say they are confident in knowing when a DPIA is required, almost a third (**31%**) are unsure.

Among organisations that do conduct DPIAs, **71%** report having processes in place to manage identified data protection risks.

Among organisations that conduct DPIAs, **69%** report that these include an assessment of the risks to individuals' rights and freedoms



JOIC Comment - Data Protection Impact Assessments (DPIA)

- The application and understanding about DPIAs is welcome
- Concerning that 2/3rds of respondents have not conducted a DPIA or DPIA style assessment and uncertainty remains about when such risk assessments are legally required.

JOIC Commitment - Data Protection Impact Assessments (DPIA)

- JOIC will continue to offer awareness sessions on this topic.
- JOIC will monitor and update our guidance on this topic where and when necessary.
- JOIC will communicate with all registered organisations to invite them to join our newsletter subscription list for frequent updates.
- JOIC will continue to encourage organisations to make use of our DPIA portal where appropriate.
- Lack of undertaking a proportionate and risk based DPIA assessment will be considered as an aggravating factor when we undertake Investigations or Inquiries.

Sharing Personal Data

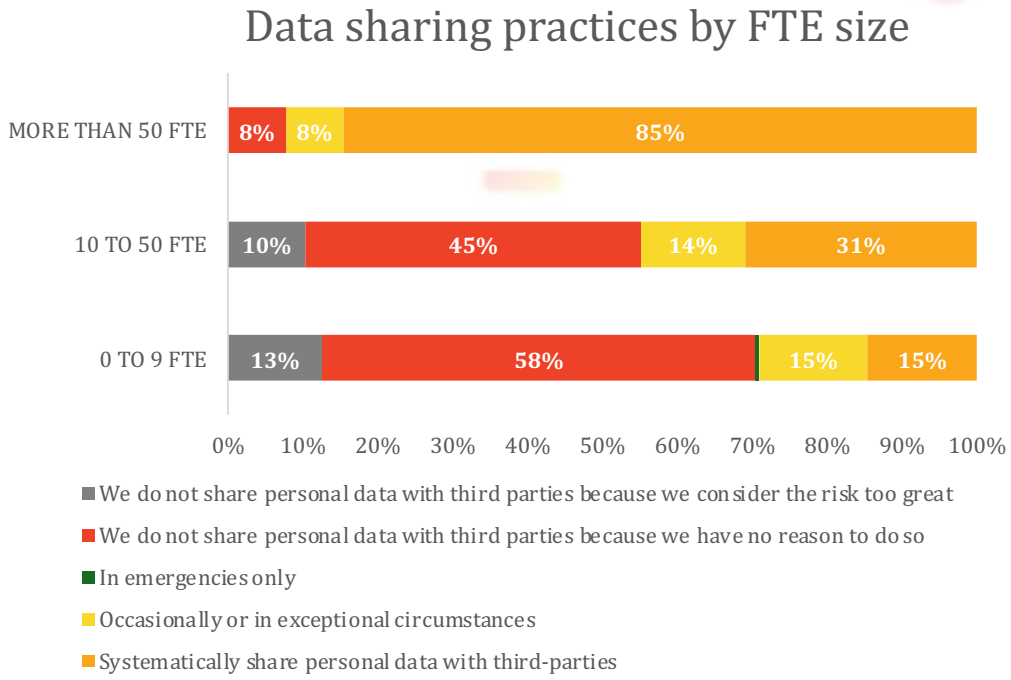
Data Sharing Practices

Two-thirds of organisations (**66%**) report that they do not share personal data with third parties, either because there is no operational need (**54%**) or due to perceived risks (**12%**).

In contrast, systematic data sharing is common among larger organisations (more than 50 FTE), with **85%** reporting they share personal data regularly with third-parties.

Overall, three-quarters (**77%**) of organisations say they are confident in sharing personal data with third parties in compliance with legislation.

A quarter (25%) of organisations that share personal data rely on data subject consent as the legal basis



Data Sharing Controls

9% of organisations report sharing personal data without any formal documentation in place.

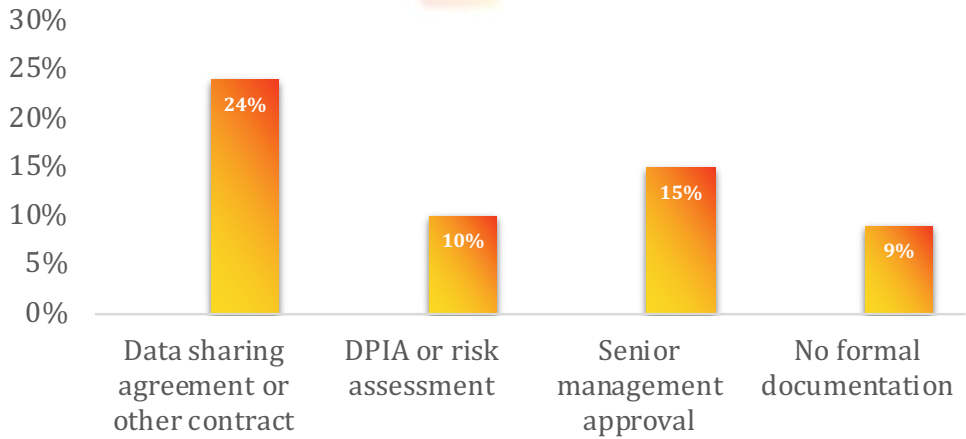
Among those with formal data sharing contracts;

- **34%** review them at least annually
- a further **27%** review them every two to five years.

Around a quarter use secure file-sharing platforms (**27%**) or password-protected documents (**24%**) when sharing personal data; adoption of technical security measures is more prevalent among larger organisations.

20% of organisations say they rely on adequacy agreements between Jersey and other jurisdictions as a safeguard when sharing personal data across borders

Types of governance used when sharing personal data with third parties



JOIC Comment – Data Sharing

- The survey highlighted that 25% of respondents rely on consent as a legal basis for transferring personal data. Given that most of those sharing data have more than 50 FTEs – consent is an unusual lawful basis upon which to rely
- Data sharing controls range from agreements or contracts to nothing formal or managerial approval
- Welcome the consideration of secure mechanisms to share personal information.

JOIC Comment – Data Sharing

- JOIC will continue to offer awareness sessions on this topic.
- JOIC will monitor and update our guidance on this topic where and when necessary, communicating any changes with industry.
- JOIC will communicate with all registered organisations to invite them to join our newsletter subscription list for frequent updates.
- Lack of training or understanding of the responsibilities of data sharing is unacceptable and is no defence when we undertake Investigations or Inquiries.

Managing Data Protection Incidents

Self-Reported Data Breaches

Two-fifths of organisations (**43%**) record all self-reported data breaches (SRDBs) regardless of severity.

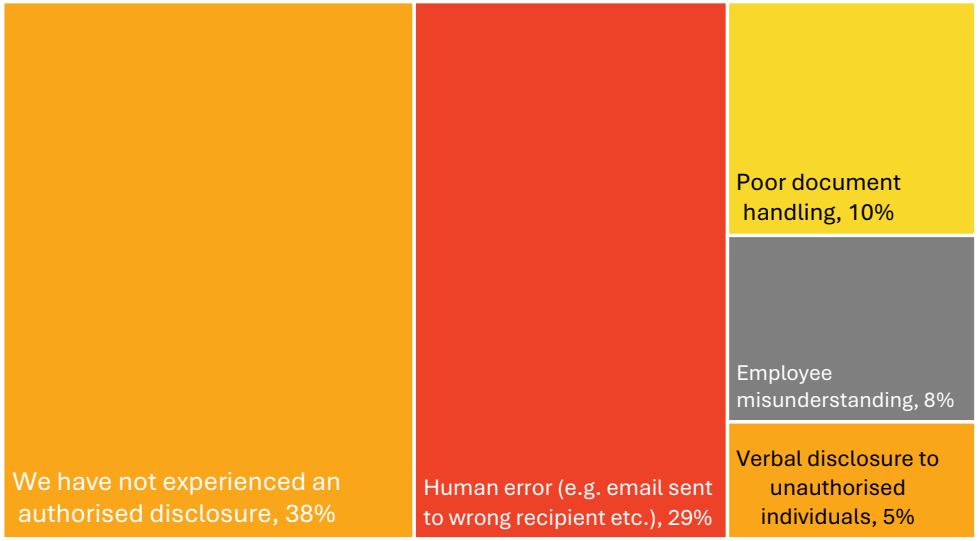
While **29%** say they keep no records.

Nearly a quarter (**23%**) of small organisations (0–9 FTE) say they have never experienced a SRDB, whereas no large organisation reported the same.

Unauthorised disclosures, including misdirected emails, incorrect attachments and verbal disclosures, are the most commonly reported type of personal data breach (**30%**).

60% of organisations say they feel confident in knowing when an SRDB is likely to pose a risk to the rights and freedoms of individuals

Main causes of unauthorised disclosure of personal data



Policies, Procedures and Controls

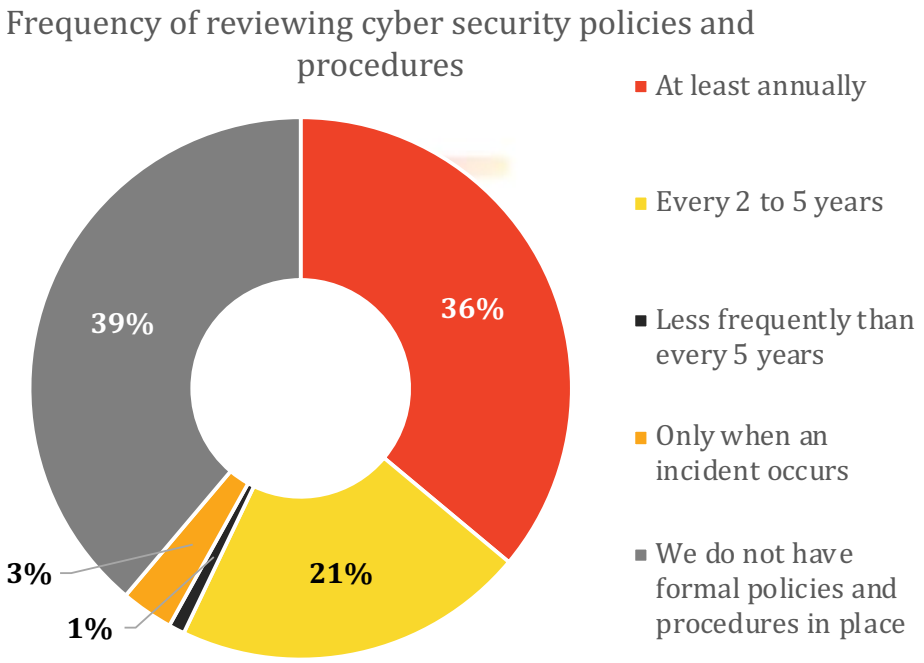
43% of organisations report using strong password requirements and/or multi-factor authentication to reduce the risk of breaches occurring.

61% review their data protection policies and procedures on a regular basis.

30% at least annually and **31%** every two to five years.

Almost two-fifths (**39%**) say they have no cyber security policies or procedures in place.

A quarter (**24%**) of organisations use end-point or anti-malware software to reduce the risk of security related breaches



JOIC Comment – Managing Data Protection Incidents

- The survey highlights that respondents (29%) are unaware of their breach recording obligations.
- Results highlight a risk in terms of the absence of cyber security procedures.
- JOIC welcome the application of MFA and strong password requirements.
- Concern 2/5 of organisations report having no formal cyber secuirty polices and procedures in place.

JOIC Commitment – Managing Data Protection Incidents

JOIC will raise awareness of breach reporting obligations and risks.

Small organisations with fewer than 10 employees say they have never experienced a data breach – JOIC will raise awareness of breaches, risks, mitigations and reporting obligations.

JOIC will monitor and update our guidance on this topic and promote such changes.

JOIC will communicate with all registered organisations to invite them to join our newsletter subscription list for frequent updates.

Lack of training or understanding of the responsibilities of data breaches is unacceptable and is no defence when we undertake Investigations or Inquiries.

Next Steps

Next Steps

- JOIC to fulfill their commitments.
- The triple AAA approach is delivering our strategic priorites, will utilise the survey results to help us deliver the priorities.

Thank you to all organisations that participated in this research.

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

enquiries@jerseyoic.org
+44 1534 716530
www.jerseyoic.org

Differences by Industry

Key Differences by Primary Industry

Data Protection Training

	Organisations (10+ FTE) that offer DP training to staff	Organisations (0 to 9 FTE) that have undertaken a formal DP training course
Agriculture, Fishing, Animal Husbandry & Welfare	70%	29%
Charities, Faith, Worship & Religion & Social Clubs	58%	56%
Construction, Trades & Services	13%	25%
Education, Childcare, Health & Wellbeing	77%	67%
Financial & Professional Services	96%	77%
Legal, Property & Professional Services	81%	44%
Leisure & Fitness, Hospitality, Tourism, Travel & Entertainment	77%	47%
Manufacturing, Wholesale & Retail	54%	20%
Media, Comms, Advertising, Tech, Utilities & Delivery Services	86%	39%
Public Authorities, Regulators & Statutory Bodies	100%	100%

Key Differences by Primary Industry

Appointing a DPO and protecting their Independence

	Organisations that have appointed a DPO	Organisations that protect their DPOs independence in policy and practice
Agriculture, Fishing, Animal Husbandry & Welfare	2%	80%
Charities, Faith, Worship & Religion & Social Clubs	8%	86%
Construction, Trades & Services	9%	93%
Education, Childcare, Health & Wellbeing	8%	76%
Financial & Professional Services	24%	41%
Legal, Property & Professional Services	19%	69%
Leisure & Fitness, Hospitality, Tourism, Travel & Entertainment	14%	70%
Manufacturing, Wholesale & Retail	1%	79%
Media, Comms, Advertising, Tech, Utilities & Delivery Services	18%	83%
Public Authorities, Regulators & Statutory Bodies	63%	29%

Key Differences by Primary Industry

AI adoption and use of DPIA style risk assessments

	Organisations that have formally adopted AI or make ad-hoc use with controls	Organisations that have never conducted a DPIA style assessment
Agriculture, Fishing, Animal Husbandry & Welfare	33%	22%
Charities, Faith, Worship & Religion & Social Clubs	54%	52%
Construction, Trades & Services	24%	24%
Education, Childcare, Health & Wellbeing	47%	29%
Financial & Professional Services	50%	84%
Legal, Property & Professional Services	51%	51%
Leisure & Fitness, Hospitality, Tourism, Travel & Entertainment	27%	50%
Manufacturing, Wholesale & Retail	34%	6%
Media, Comms, Advertising, Tech, Utilities & Delivery Services	30%	62%
Public Authorities, Regulators & Statutory Bodies	88%	86%