Data Protection Competency Framework

Competency – a behaviour that can be acquired through learning, and demonstrated in practice.

Licensing

Version v1.0

Version	Author	Date	Approved by	Effective from
1.0	Rowenna Fielding	1 April 2021	James England	1 May 2021

Contents

About this framework

Introduction

Data Protection Education is pleased to issue this Data Protection Competency Framework.

We commissioned this work from Miss IG Geek because we wanted another set of eyes on an important, but seemingly missing piece of the data protection jigsaw - that is the human element.

We often hear our colleagues, customers and ourselves say that "people are the biggest risk" and we see this daily - systems security in place, but defences and data breached through human error or deception. But the human factor goes beyond the risk of a phishing attack - it's about roles throughout the organisation.

In data protection law the organisation has accountability, but organisations are made of people. Therefore, ensuring that your people understand their role and what it requires of them to ensure the organisation as a whole has an effective data protection programme is key. It isn't simply the role of the IT department or the office administrator - everyone has a role.

That's why this framework is so valuable - it's not just a set of skills and attainments. Rather, it looks at what different roles exist in data processing and assigns the competency to that role, understanding that in different processing activity, people may be doing different things.

We commissioned this work because we wanted to map roles effectively in our record of processing activity tool and when conducting data protection impact assessments. This framework allows us to provide staff with a personalised report and learning plan based on what they actually do. After all, if people are the biggest risk, we have to put them at the heart of the data protection risk management framework.

We've made this data protection competency framework available under a creative commons licence because we want you to use it, benefit from it and develop it for your needs.

We'd love to hear from you about how you use and adapt it in your organisation and industry. That means send us your ideas, suggestions for improvement and any adaptations that you make - we really want to see this grow across the community.

James England

Director

Data Protection Education Ltd.

What’s this framework for?

The purpose of this framework is to establish an initial, baseline set of competencies for data protection which are industry- and sector-neutral, so that it can be adopted "as is", without requiring significant effort to map the competencies to specific role titles or functions.

It describes behaviours that support compliance and good practice in data protection so that individuals can acquire and demonstrate their maturity in this area; and organisations can build training programmes and performance metrics that relate to practical, real-world actions.

There is no "one size fits all" approach to data protection, as so much of its decision-making and activities are dependent on an organisation’s approach to risk, ethics or regulation; so this framework is designed to support foundational compliance efforts without dictating *how* specific activities should be carried out.

Who can use it?

- Any organisation which is seeking to improve or maintain its compliance with data protection law.
- Organisations that recognise the competitive advantage of effective data protection management
- Trainers devising learning programmes for practical data protection
- Individuals seeking to add value to their personal profile for employers by demonstrating data protection competencies
- Quality, governance and compliance functions seeking to measure and quantify data protection competencies

What if…

…my organisation doesn’t have the policies, standards, governance structures or other management tools mentioned in this framework?

In addition to building and measuring individual competencies, this framework can also be used as a gap-analysis and guide for *organisational* competency in data protection, as it identifies key structures and systems for data protection management which are necessary to support good practice (and in some cases, essential for compliance with the law).

If an individual competency cannot be demonstrated because it relies on corporate infrastructure or governance that isn’t in place, the competency cannot be fairly assessed. When tracking and recording competencies using this framework, these gaps must be accurately logged as systemic/structural barriers to achievement, so that the individual is not wrongly characterised as 'failing' to demonstrate the competency.

Why are there no attainment levels to assess against?

There is so much variation in grades of seniority, authority and autonomy across organisations, that designing fair and practical attainment levels which mapped data protection competencies consistently to those variations turned out to be a significant challenge! What one organisation would consider basic/intermediate/advanced competencies for data protection may not be at all suitable for a different organisation, and rather than try to stuff people into boxes that are the wrong shape for their roles, we've decided to design the framework around different aspects of people's involvement with the processing of personal data instead. This means that people can adopt the competencies that are relevant in practice to their roles, and not worry about performing to an arbitrary standard of achievement that doesn't fit with their day-to-day work.

Almost everyone in an organisation is likely to be an **Info Handler** to some degree – whether the personal data being handled is that of fellow employees, customers, the general public or professional connections.

Business Process Owners are individuals within an organisation who decide how things should be done, and why. For example, an HR Manager will own business processes for payroll, recruitment, onboarding, occupational health, etc – even if they don't carry out the processing of personal data themselves or directly supervise the people following the process. If someone must be asked for authorisation to change the way an activity is carried out; that person is the business process owner.

Executives are the top tier of management, who make the big decisions about what the organisation exists to do, and how it is structured.

The **Data Protection Officer (DPO)** is a specialist in data protection, who advises and supports the organisation on compliance with data protection law and good practice. A DPO has a professional obligation to maintain their data protection expertise. Not all organisations will need to have a statutory DPO (as defined by Article 37 of the GDPR), but those which do will need to be able to demonstrate that the role is being appropriately fulfilled.

ICT Providers are any staff, internal or outsourced, who are responsible for providing, sourcing, supporting or maintaining digital and communications technology for the organisation. Although data protection is not specific or limited to digital and electronic systems; many of the risks, controls and decisions that data protection relies on, will involve technology to some degree, and require input from technology specialists.

What's inside?

The framework is organised into three domains for data protection competency – **Business & Law, Technology and Tools, People and Values**, which cover all aspects of data protection practice and management that an organisation needs to consider.

Each domain has an area of practice, and within these areas are particular focus topics.

Every competency is defined by a "You" statement, which describes a behaviour that relates to good practice in data protection. To be helpful, we've identified some ways in which the behaviour can be demonstrated and supported with evidence, however these should not be viewed as exhaustive or prescriptive. Organisations and individuals are free to add their own ideas for demonstrating and measuring these competencies.

Licensing

The framework is provided under a 'CC-BY-NC' Creative Commons license type, which means that anyone is free to reuse, re-mix, adapt and build on the original content in any format or medium, but *only* for non-commercial purposes, and *only* as long as Data Protection Education Ltd and Miss IG Geek Ltd are credited for the original content.

Using the framework effectively: dos and don'ts

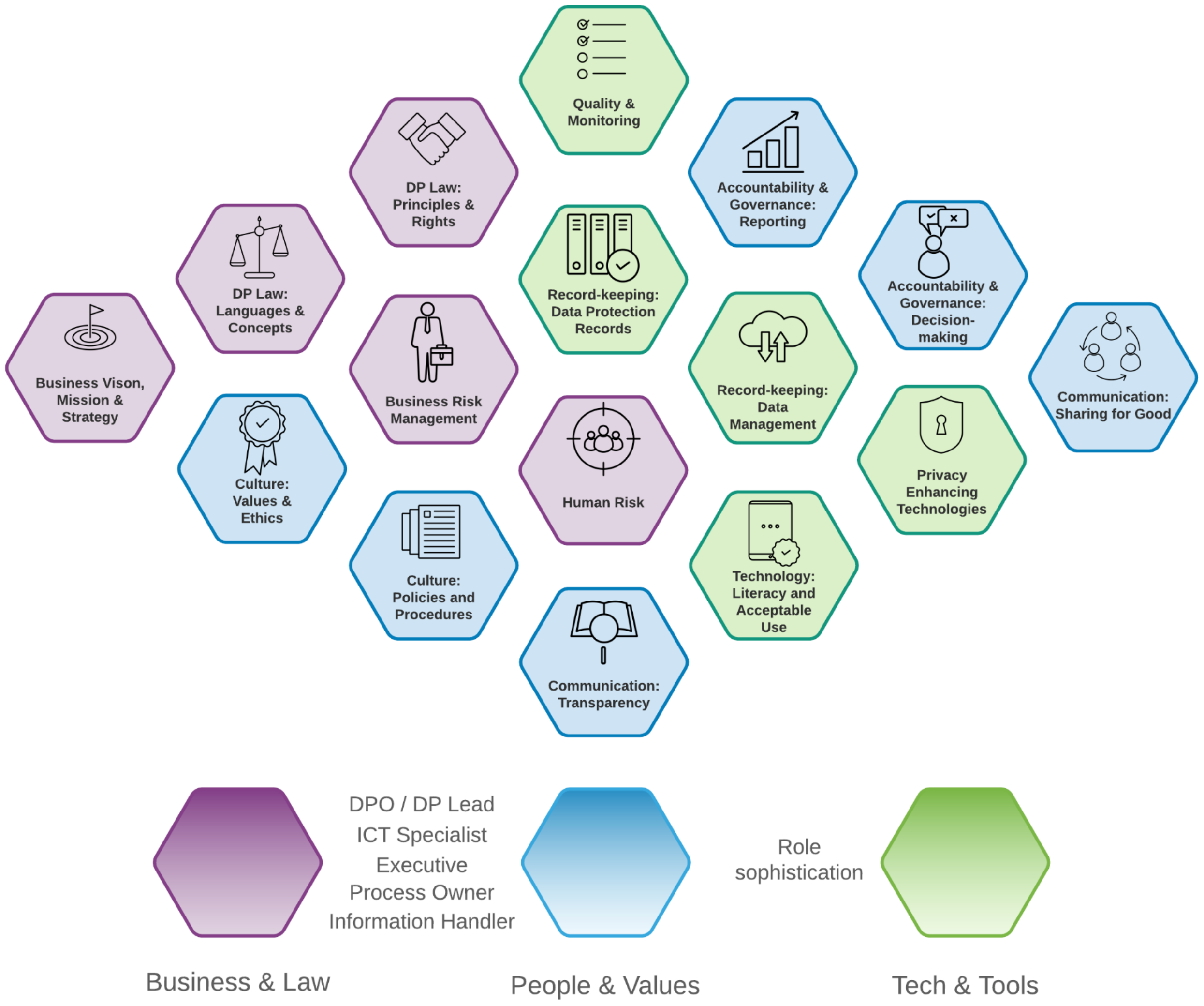
Do

- integrate the framework into medium- and long-term strategies
- examine the requirements from an organisational viewpoint first – are the governance structures in place? Do learning resources and support tools exist?
- make time and space for the *thinking* that will need to be done in order for the framework to be adopted successfully. Be realistic about the timeframes and person-power that will be required to prepare for, roll out and make use of the framework as part of business-as-usual.
- pick out the bits which are useful to your organisation, or to you as an individual.
- adapt, innovate, develop and contribute to future iterations of the framework – diversity of input makes for quality of output!

Don’t

- impose the framework as a set of ‘all or nothing’ requirements from the outset, or set arbitrary time limits for ‘passing’ or ‘completing’ it. These approaches are likely to drive counterproductive activities, such as ‘box-ticking’, or ‘gaming’ the demonstration part, to produce a cosmetic appearance of good practice without any of the benefits.
- treat the implementation of the framework as a one-time ‘fire and forget’ activity. Behaviours must be continually practised and affirmed in order to become habits, especially when they introduce friction or lead away from the path of least resistance.
- breach the licensing terms, please

The Framework


Quality & Monitoring
DP Law: Principles & Rights
Accountability & Governance: Reporting
DP Law: Languages & Concepts
Record-keeping: Data Protection Records
Accountability & Governance: Decision-making
Business Vison, Mission & Strategy
Business Risk Management
Record-keeping: Data Management
Communication: Sharing for Good
Culture: Values & Ethics
Human Risk
Privacy Enhancing Technologies
Culture: Policies and Procedures
Technology: Literacy and Acceptable Use
Communication: Transparency
DPO / DP Lead
ICT Specialist
Executive
Process Owner
Information Handler
Role sophistication
Business & Law
People & Values
Tech & Tools

Business & Law

Vision, mission, strategy

Role	Competency	Suggestions for demonstrating this competency
Info Handlers	You recognise and promote the benefits of good practice in data protection; for your organisation, data subjects and wider society.	● Use positive language about data protection. ● Acknowledge commercial and operational benefits of robust data protection. ● Acknowledge individual and social benefits of data protection.
Business Process Owners	You play an active role in aligning business practices with data protection obligations.	● Show that DPIAs are routinely considered/carried out for changes or new activities under your supervision. ● Refer to data protection in terms of support for human rights and freedoms (not a barrier or burden to business). ● Query/raise concerns when working practices are not aligned with data protection requirements.
Executives	You frame robust data protection practices as a strategic enabler when addressing your organisation's compliance position and operational standards.	● Set thresholds for data protection strategy above 'cosmetic compliance' or 'bare minimum'. ● Articulate the benefits of good practice to your organisation, society and individual rights and freedoms.

DPO	You advise on where and how good data protection practices can support the delivery of the organisation's vision, mission and strategy.	● Provide advice, guidance and steering without hijacking business decisions. ● Contribute your expertise to finding solutions, as well as identifying problems. ● Build a reputation for being the Department of Doing This Safely, (not the Department of 'No').
ICT	You seek to align and balance conflicts of interest between ICT objectives and data protection compliance.	● Be able to explain describe, in basic terms, the differences and overlaps between data protection and information security . ● Avoid positioning privacy and security, or privacy and functionality as antagonists when discussing protective measures.

Data Protection Law

Language and Concepts

Role	Competency	Suggestions for demonstrating this competency
Info Handler	You understand and use key data protection terms correctly when they are relevant to your role.	● Check and refresh your understanding of data protection language; particularly "personal data", "processing", "Controller", and "lawful basis". ● Find and familiarise yourself with guidance on how to recognise a data subject rights request, and what you should do if you encounter one.
Business Process Owner	You can describe the purposes and lawful bases of the processing activities which come within your area of responsibility. You take steps to create and maintain evidence requirements to support your organisation's lawful processing.	● Contribute this information to the Records of Processing Activity (ROPA). ● Carry out a Purpose Compatibility Assessment when seeking to re-use personal data for a new purpose. ● Allocate preparation time and resources to reviewing and establishing a lawful basis when making changes to processing activities within your remit.

Executives	You play an active role in aligning organisational strategy and governance arrangements with the requirements of data protection law.	● Play an active role in data protection governance/risk management activities. ● Engage with organisational resources for data protection learning and guidance.
DPO	You maintain advanced knowledge of regulatory guidance, legislation and case law relating to data protection which is relevant to your organisation’s industry or sector.	● Keep yourself apprised of developments in case law and regulatory guidance. ● Discuss industry/sector-specific aspects of data protection with peers and colleagues in the field.
ICT	You take steps to avoid misunderstandings of data protection language that has different meanings than from ICT industry/professional uses.	● Signpost or provide the definitions or interpretations you are relying on when using terms such as "archiving", "processing, "data", "‘policy" or "identification". ● Verify the intended meaning when encountering these terms in your role.

Principles and Rights

Role	Competency	Suggestions for demonstrating this competency
Info Handler	You look for ways to apply the data protection Principles to your working practices, recognising and responding appropriately to data subject rights requests.	● Handle personal data with care and attention. ● Check before re-using personal data for a new purpose. ● Make use of resources that tell you how to recognise and handle data subject rights requests. ● Ask questions about why and how personal data is processed. ● Report any concerns.
Business Process Owner	You take steps to integrate data protection by design and by default as a core component in the business processes you are responsible for .	● Access learning and resources on "Data Protection by Design and by Default". ● Require Data Protection Impact Assessments to be considered for changes to processing or new processing activities. ● Allocate suitable resources to data protection activities so that they can be routinely carried out within 'business as usual' parameters. ● Take ownership of data protection risks that occur within your remit.
Executives	You uphold and affirm data protection principles and rights within your leadership role.	● Lead by example in adhering to policies and procedures, and making use of learning and support resources. ● Require a data protection impact assessment before approving the adoption of any type of productivity monitoring or workplace surveillance.

		● Show respect for the data subject rights of the organisation’s workforce.
DPO	You prompt and assist your colleagues to give data protection principles and rights due consideration in all organisational activities.	● Provide materials that encourage and support the adoption of privacy/data protection culture within the organisation. ● Review organisational processes and procedures to identify where ‘think about data protection’ checkpoints can/should be introduced.
ICT	You pay attention to the protection of data subject rights and adherence to all data protection principles (not just security) when providing ICT services.	● Prompt colleagues to conduct a Data Protection Impact Assessment when you provide ICT input to projects or changes ● Include criteria for protection of data subject rights and adherence to data protection principles when assessing new providers or tools. ● Assist with retrieving data for subject rights requests. ● Provide tools and/or support for data minimisation and deletion.

Risk Management

Business Risk

Role	Competency	Suggestions for demonstrating this competency
Info Handler	You recognise and work within organisational controls for managing data protection risk.	● Access organisational policies and ask for an explanation of any aspect that isn't clear ● Raise concerns when you encounter gaps between organisational policy and operational requirements.
Business Process Owner	You pay attention to data protection risks and contribute to measures necessary to prevent them from turning into issues.	● Identify data protection risks early in the design and planning stages for new or changing business processes. ● Don't hide from the DPO
Executives	You encourage and model an effective risk management approach.	● Engage proactively with risk management and governance activities (i.e. don't just delegate everything data protection-related). ● Identify and communicate organisational tolerances for acceptable risk. ● Allocate adequate resources for monitoring and maintaining risks within tolerances.

DPO	You provide insight on data protection risk exposure and prioritisation to corporate risk and governance bodies, allowing senior management to make informed decisions about managing those risks.	● Identify and communicate data protection risks. ● Advise on how risks to data subjects' rights and freedoms relate to business risks. ● Advise the organisation when data protection risks may exceed tolerances. ● Provide guidance on mitigating or avoiding excess risk.
ICT	You recognise and routinely consider ICT risk factors relating to data protection.	● Maintain awareness of digital privacy issues and developments. ● Liaise with the DPO to align ICT activity with the management of data protection risk.

Human Risk

Role	Competency	Suggestions for demonstrating this competency
Info Handler	You can describe, or give examples of, ‘human risks’, and recognise how/when they might arise.	● Make use of learning resources about human rights and privacy risks. ● Engage with discussions or consultations about business ethics.
Business Process Owner	You consider potential and actual conflicts between business and human risk when developing or supervising processes, and resolve these conflicts according to organisational policy and risk tolerances.	● Encourage the use of Data Protection Impact Assessments as a critical data protection risk management tool. ● Refer to organisational policies and risk statements when addressing data protection risks. ● Document risk-conflict decisions.
Executives	You give human risk due consideration in setting strategic policy and operational priorities for data protection.	● Establish an ethical stance that sets out tolerances for human risk, harm avoidance and thresholds for action. ● Routinely consider and document potential human risks when conducting planning or strategy sessions.

DPO	You provide the organisation with expert analysis and advice on managing human risk alongside business risk.	● Monitor and report individual and aggregate human risk assumed by the organisation for data processing activities. ● Recommend options and tactics for balancing human risk with business risk. ● Maintain awareness of human risks presented by current and developing technologies.
ICT	You maintain awareness of human risk implications in design, development, procurement operation and support of ICT services.	● Engage with the DPO to assess the human risk of ICT designs, development, procurement and support. ● Conduct Data Protection Impact Assessments on the use of technologies that have high associated human risks, such as surveillance tools, predictive algorithms, biometric analysis, and automated decision-making. ● Seek out information and updates about human risks arising from developing technologies.

Tech and Tools

Assurance

Quality & Monitoring

Role	Competency	Suggestions for demonstrating this competency
Info Handler	You keep an eye out for potential data protection problems and resolve or escalate issues when you notice them.	● Check the quality and accuracy of personal data you work with as part of your routine activities.
Business Process Owner	You foster a fair and consistent approach to risk and problem reporting.	● Accept risk or problem reports that relate to your business processes, and focus on solutions, without seeking to silence, discredit or retaliate against the person reporting. ● Seek to identify and resolve systemic aspects of risks and problems that arise. ● Give preference to sustainable, effective actions to resolve risks or problems, even when superficial cosmetic changes are quicker, cheaper or easier.

Executives	You seek to mitigate systemic factors which present barriers to data protection quality and compliance.	● Acknowledge and mitigate environmental conditions which prompt or enable risky behaviour, without seeking to silence, discredit or retaliate against individuals. ● Identify and correct systemic, structural barriers to good data protection practice before apportioning culpability to individuals' actions.
DPO	You use data protection monitoring and reporting as intelligence-gathering tools to help the organisation manage risk.	● Set or recommend metrics for measuring the uptake and effectiveness of data protection measures. ● Provide regular reporting to senior management on the organisation's data protection compliance status, maturity level, (potential) trouble spots and effectiveness of data protection controls. ● Identify issues that undermine the organisation's ability to keep data protection risk within acceptable limits.
ICT	Where you provide ICT support and/or services for measurement, tracking and reporting of performance or quality; you do so without excessive surveillance or unwarranted intrusion on individual privacy.	● Require a DPIA to be conducted for any implementation of compliance monitoring which involves automated surveillance of employees. ● Advise on the assumptions and limitations of tools used to track and report risk and compliance, so that their output can be evaluated in context. ● Distinguish between information security tools and privacy compliance tools to prevent inappropriate use.

Record-Keeping

Data Protection Records

Role	Competency	Suggestions for demonstrating this competency
Info Handler	You can describe how your organisation's data protection record-keeping requirements relate to your role.	● Identify which elements of data protection and records management policy or procedure apply to your working activities. ● Check that you are equipped with the knowledge and tools required to put policy and procedure into practice. ● Integrate data protection record-keeping into your tasks and business-as-usual workload.
Business Process Owner	You make use of the organisation's Records of Processing Activities; setting a good example of data protection record-keeping in your own activities.	● Notify the owner of the ROPA of/update the ROPA with any new recipients of personal data, changes to systems or processing activities, additions of new data or changes to the retention of personal data for the activities you are responsible for. ● Consider data protection record-keeping requirements when planning and making changes.

Executives	You identify and allocate adequate resources to maintaining essential record-keeping activities while leading good practice by example.	● Consult with the DPO and ICT staff on dependencies for record-keeping activities, and factor these into plans, budgets and schedules. ● Comply with organisational policies and procedures for data protection and records management, even when doing so seems inconvenient to you.
DPO	You can advise on the appropriate data protection record-keeping activities required for the organisation to meet its obligations in data protection law, regulatory cooperation and transparency.	● Conduct spot checks on the ROPA to check that it's up to date. ● Audit contract record-keeping and terms. ● Maintain or evaluate staff training records for data protection. ● Advise on keeping track of privacy notices, audit PN record-keeping.
ICT	You uphold and enable effective record-keeping by factoring its requirements into the design, procurement and operation of ICT.	● Maintain, or contribute to, centralised records of agreements with third party ICT suppliers. ● Integrate 'update the ROPA' checkpoints into ICT change control and project management materials and processes. ● Assist the DPO in identifying suitable compliance tracking and case/incident management tools as needed.

Data Management

Role	Competency	Suggestions for demonstrating this competency
Info Handler	You organise and manage your individual data stores in line with organisational standards and comply with procedures for managing data in shared data systems.	● Regularly delete redundant, outdated and trivial content from your mailbox and file stores. ● Use consistent file naming and version controls for items in shared data storage locations. ● Avoid making local copies of shared documents whenever possible; link to shared files instead of attaching them, use collaboration functions where available.
Business Process Owner	You make provisions for suitable data management resources within the business processes you oversee.	● Ascertain and include the time and effort of checking and maintaining data stores in business planning and resource allocation. ● Accept, or assign responsibility for conducting data provenance checks and due diligence on new sources of personal data.
Executives	You recognise and factor the organisation's data management needs into technology strategies and planning.	● Consider and account for human factors in data management (time, cognitive load, access, training) when setting strategy for new ways of

		working, or adopting new technologies.
DPO	You use your knowledge of the organisation, data protection law and good practice to offer constructive recommendations on data management practices.	● Give advice based on the organisation’s capabilities and risk tolerances. ● Be alert for suggestions or plans of using "A" or "machine learning" to classify or manage data stores to ensure that outliers, error rates and exception handling are considered. ● Maintain awareness of industry or sector guidelines for data management that are relevant to your organisation.
ICT	You support and facilitate effective data management among colleagues.	● Consider user experience, and future-proofing when assessing tools or technologies to assist with data management. ● Provide input and assistance to data management decisions and plans. ● Ask for specifics of data management or functionality requirements when tasked with identifying suitable systems or tools.

Technology

Tech Literacy & Acceptable Use

Role	Competency	Suggestions for demonstrating this competency
Info Handler	You use workplace technologies safely and securely.	● Check with ICT and the DPO before installing or signing up to use any ‘free’ tool or service for work purposes. ● Refer and adhere to your organisation’s policies and procedures for information security and acceptable use. ● Make use of guidance and learning resources for workplace technologies.
Business Process Owner	You seek advice and consider risks before introducing new technologies or changes to how technology is used.	● Start data protection risk assessments or DPIAs early on in designing or planning the adoption of new technologies, and ensure they are updated throughout the lifetime of the changes. ● Consider and document human factors which might result in unsafe or inappropriate use of workplace technologies. ● Establish required specifications, functions and privacy-safe requirements *before* evaluating or testing specific products or services.

Executives	You make provisions for improving/maintaining appropriate staff tech literacy across the organisation.	● Invest in programmes and resources for staff tech literacy and safe, acceptable uses of technology. ● Solicit and consider feedback on barriers to effective, safe uses of technology and systems.
DPO	You maintain awareness of data protection risks and controls arising from technology developments and uses.	● Make use of resources for understanding and implementing "data protection by design and default". ● Follow news and research on privacy risks of new and developing technologies such as machine learning, biometric analysis, and predictive algorithms.
ICT	You support and enable improvements in tech literacy among colleagues.	● Suggest or contribute resources for improving tech literacy. ● Consider and account for human factors (time to adapt, cognitive load, accessibility, training) when planning significant changes to technologies already in use within the organisation. ● Signpost or make resources for learning tech literacy available to colleagues.

Privacy-Enhancing Technologies (PETs)

Role	Competency	Suggestions for demonstrating this competency
Info Handler	You make use of Privacy-Enhancing Technologies where they are available.	● Protect confidential information with encryption when transmitting it outside the organisation.
Business Process Owner	You give consideration to the benefits of PETs.	● Actively encourage consideration of appropriate PETs as part of data protection by design and default, when planning or making changes to business processes you oversee.
Executives	You are willing to consider the value of recommended PETs in terms of human risk and ethics, alongside financial cost.	● Engage with the findings of DPIAs and risk assessments.
DPO	You advise the organisation on when/how there is value to deploying PETs.	● Learn the basic functions, benefits and limits of PETs and ICT security technologies, in particular; encryption, authentication, access control, privilege management, logging/monitoring, differential privacy and tokenisation so that you can incorporate this knowledge into risk assessments and recommendations.

ICT	You use your knowledge of PETs to support colleagues in making safe, compliant use of ICT resources.	● Generate 'dummy' data instead of using live personal data for testing and development activities. ● Consider the use of tokenisation instead of direct end-user access to personal datasets ● Produce accessible guidance and documentation on the correct use of PETs within the organisation.

People and Values

Accountability & Governance

Decision-Making

Role	Competency	Suggestions for demonstrating this competency
Info Handler	You obtain advice from the DPO to inform your own decision-making, rather than expecting them to make decisions on your behalf.	● Know and reference organisational policy and guidance on data protection when making decisions. ● Seek input and recommendations (not sign-off, or authorisation) for your decisions.
Business Process Owner	You make decisions with data protection as a key aspect from the start, rather than attempting to add it on later.	● Consult data protection guidance or the DPO early on in decision-making so that "data protection by design and by default" can be incorporated effectively. ● Record and justify decisions where data protection requirements have been discounted or superseded.
Executives	You accept accountability for making business decisions that have data protection implications.	● Frame data protection as a contribution to decisions, not an antagonist (eg "how do we do this safely and legally?", not "is this against data protection rules?"). ● Where you have over-ruled or declined the DPO's

		recommendations, account for this decision in writing so that it is reflected in organisational records.
DPO	You balance your organisation's support needs with your professional obligations, including the need to avoid conflicts of interest with your DPO role.	● Describe options, explanations and recommendations for meeting data protection requirements in day-to-day working as well as plans or strategies. ● Inform, rather than usurp, colleagues' decision-making. ● Communicate clearly that your role is to guide, monitor and advise on data protection risk; not to dictate business operations.
ICT	You consider the "bigger picture" of the organisation's data protection obligations and goals when making ICT decisions.	● Seek to align (not "win victory over") data protection requirements with those of ICT security and functionality.

Reporting

Role	Competency	Suggestions for demonstrating this competency
Info Handler	You report data protection incidents, breaches and problems promptly through the appropriate channels.	● Access resources on how to recognise data protection incidents, breaches and problems. ● Seek out guidance on reporting in advance, so you know how to find it in time-critical circumstances. ● Proactively report near-misses as well as actual incidents.
Business Process Owner	You encourage and support reporting of data protection risk, concerns or problems; and engage constructively with data protection reporting.	● Include steps or signposting for data protection reporting as part of the business processes you oversee. ● Recognise that most data protection issues are the result of unintended or unforeseen consequences, and therefore frame reporting as ‘identifying improvements’ (rather than ‘snitching’ or casting blame). ● Responding swiftly and constructively to reports relating to data protection issues.

Executives	You pay attention to data protection reporting and are open to hearing about risks, improvements or concerns.	● Identify and communicate organisational tolerances for acceptable risk. ● Include data protection risk reporting as a standing agenda item for regular governance meetings. ● Support and encourage honest reporting of data protection issues. ● Avoid scapegoating or punishing staff for reporting issues and concerns.
DPO	You monitor and report to senior management on the organisation's data protection compliance and risk positions, advising on severity, imminence and remedial actions. You act as liaison with the regulator for reporting breaches, responding to enquiries and demonstrating the organisation's compliance position.	● Identify suitable metrics for reporting data protection risk, and present them with audience-appropriate explanations. ● Use incidents and concerns to illustrate the benefits of working towards data protection maturity levels, rather than reacting to issues as they arise. ● Maintain professional integrity when reporting to the regulator, providing comprehensive and accurate information.
ICT	You facilitate the collection and/or generation of risk and performance reports for data protection without compromising the organisation's own compliance position.	● Require a DPIA to be conducted before implementing any kind of automated workplace surveillance or performance-monitoring tool.

Communication

Transparency

Role	Competency	Suggestions for demonstrating this competency
Info Handler	You can explain how and why you are processing personal data. You recognise data subject access requests and know what steps to take when you encounter one.	● Be able to signpost to, and explain your organisation's privacy notices in relation to the processing of personal data you carry out in your role.
Business Process Owner	You take steps to update and maintain privacy information provided to data subjects.	● Include checkpoints for reviewing relevant privacy information when making changes to processes and procedures.
Executives	You recognise transparency obligations (privacy information, consent management) as an opportunity to effectively communicate important information to data subjects.	● Establish and embed organisational strategy and standards for accessibility of privacy information.

DPO	You can explain and advise on good practice for meeting Article 12 requirements for transparency.	● Factor in accessibility, audience-appropriate language and ‘house style’ when reviewing privacy notices. ● Consult with data subjects on comprehensibility and user experience of the organisation’s privacy information. ● Maintain up-to-date knowledge of good practice in delivering privacy information.
ICT	You can explain the functions and purposes of ICT which is used to process personal data, in language that non-ICT specialists can understand.	● Provide accessible information on data flows and processing components. ● Recognise, and challenge organisational uses of "dark patterns".

Sharing For Good

Role	Competency	Demonstration
Info Handler	You only disclose personal data outside your organisation when you are confident that doing so is necessary and lawful.	● Be able to explain the purposes, lawful basis and objectives of disclosures ('data sharing') that you participate in.
Business Process Owner	You only direct, or permit, personal data to be disclosed outside the organisation when you are confident it will be done so safely and lawfully in practice.	● Set terms for external disclosures *before* the data is handed over/sent out/made available, and check that these terms are adhered to. ● Consider and make adequate provisions for safe and suitable disclosure (secure transmission, training, procedures) when planning or overseeing activities that (may) require disclosure of personal data outside the organisation.
Executives	You are realistic and circumspect about the level of resourcing necessary to carry out disclosures safely and lawfully, incorporating these requirements into planning and budgeting.	●

DPO	You can provide competent practical advice on whether a disclosure of personal data is fair and lawful, taking into account the legal gateways and restrictions that are relevant to the organisation's operating environment.	● Access continuing professional development resources for data protection law and practice updates in relevant areas. ● Network and learn from peers in the same, or related areas of industry to collaborate on examples of good practice.
ICT	You understand and can explain, technologies that may support or undermine safe and lawful sharing of personal data.	● Consider human factor challenges such as user experience and accessibility when proposing technologies for safe and lawful sharing. ● Use plain non-technical language, analogies and storytelling to explain the functions and limitations of proposed technologies.

Culture

Policies & Procedures

Role	Competency	Demonstration
Info Handler	You are diligent and careful about adhering to your organisation's policies and procedures.	● Identify and describe how policies and procedures relate to your working activities. ● Find out where policies and procedures are published, and refer to them frequently. ● Send feedback to policy and procedure owners to help optimise their content and presentation.
Business Process Owner	You write clear, accessible policies and procedures which are aligned with data protection requirements and effective in practice.	● Solicit and incorporate feedback on policy/procedure content and presentation before publishing. ● Use "plain English" checking tools, and avoid overly formal or jargon-heavy language.
Executives	You establish a data protection policy by evaluating and communicating an appropriate balance of legal, operational, commercial and ethical risk for your organisation.	● Set aside time to discuss and consider why and how policy can be formulated for effectiveness. ● Treat policy documents as a tool first, and a weapon second. ● Enforce policy consistently and fairly.

DPO	You can identify where policy and procedure content raises barriers to, or undermines data protection requirements, and collaborate effectively to resolve these issues.	● Offer input early and throughout policy/procedure development processes. ● Provide constructive feedback and assistance in helping to align policy content with data protection compliance requirements.
ICT	You consider and integrate the requirements of data protection policy and procedures into ICT procurement, configuration and service delivery.	● Comply with organisational policies and standards for procurement. ● Access resources for learning about "data protection by design and by default". ● Keep a lookout for conflicts and contradictions between ICT activities and data protection policy.

Values & Ethics

Role	Competency	Demonstration
Info Handler	You take steps to keep your working practices aligned with the organisation's values and ethics.	● Risk-assess shortcuts and conveniences with values and ethics in mind. ● Take steps to keep in mind that 'personal data' represents real, living humans. ● Politely and professionally challenge practices that are out of step with the organisation's stated values and ethics.
Business Process Owner	You include consideration of organisational values and ethics when making decisions that relate to the processing of personal data.	● Approach "compliance" as a minimum requirement that can be built upon, rather than a fixed ceiling for attainment. ● Access resources for learning about "data protection by design and by default".
Executives	You establish the organisation's values and ethics, lead by example in demonstrating them; and are open to feedback on the effectiveness of these measures.	● Include values-based behaviours and ethical standards in quality and performance monitoring ● Consider adopting a "Just Culture[1]" approach to data protection. ● Consider aligning data protection initiatives with programmes addressing inclusivity, accessibility,

[1] https://en.wikipedia.org/wiki/Just_culture

		corporate social responsibility and environmental impact.
DPO	You reference the organisation's stated values and ethics in addition to compliance requirements when providing data protection advice or learning materials.	● Identify and explain where proposals or practices relating to personal data processing are in conflict with the organisation's stated values and ethics. ● Use inclusive language in guidance and learning materials, and provide them in disability-accessible formats.
ICT	You give strong consideration to accessibility and sustainability according to your organisation's stated values and ethics when making decisions about ICT supply or provision.	● Give preference and priority to suppliers in locations deemed "adequate" under data protection law. ● Highlight and advise where ICT requirements cannot be met without falling short of organisational values and ethics.

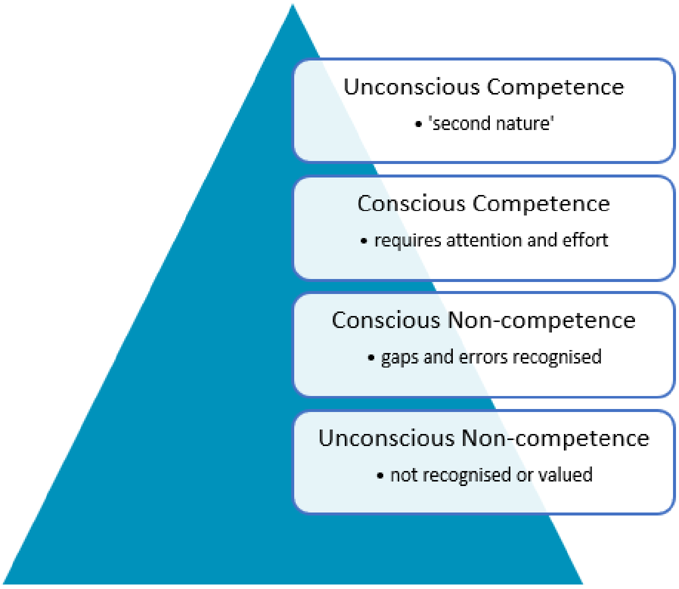
Assessing staff competencies against the DPCF.

Although it would be optimum for all staff to be able to keep in mind and carry out their data protection obligations at all times; realistically, there will be many factors that prevent them from doing so. These are likely to include:

- Insufficient available time for learning and development, re-engineering of processes, evaluation and planning
- Conflicts between operational requirements ("get this done ASAP") and compliance requirements ("do this *right*")
- Cultural barriers to adoption (“oh no, not another framework/standard/checklist/etc to have to cope with”)
- The steep learning curve for gaining the knowledge required to demonstrate the competencies
- Lack of organisational resources or infrastructure preventing staff from demonstrating their competencies

In order not to overload staff or provoke resistance to adoption of the Framework, we advise being pragmatic and transparent about these environmental factors and recommend using the DPCF to address improvements in these areas *before* attempting to measure or formally apply competency requirements.

The Four Stages of Competence[2]:


Unconscious Competence
• 'second nature'
Conscious Competence
• requires attention and effort
Conscious Non-competence
• gaps and errors recognised
Unconscious Non-competence
• not recognised or valued

[2] https://en.wikipedia.org/wiki/Four_stages_of_competence

As data protection law has only recently been strengthened, and most organisations will have a large amount of "compliance debt" to catch up on, it is reasonable to assume that most people in the organisation will be somewhere between "unconscious non-competence" and "conscious non-competence" for many of the competency areas outlined in this framework.

Although, working towards "unconscious competence" for all staff in all applicable competencies is a laudable goal, in practice it is unlikely to be attainable. However, provided that data protection competencies can be adapted into organisational culture and practices, sustained through management supervision and support, adequately resourced and positively reinforced; a level of "conscious competence" in data protection should be possible for the majority of staff to reach. Much of the likelihood of success will depend on the organisation’s appetite for investing in resources such as learning materials, knowledge management, coaching and external expertise.