dpo.ie
the association of
data protection officers

ICS

Data Protection by Design

Making it Effective
A guidance paper

Document Authors:
Working Group of the Association of Data Protection Officers

Head of Working Group:
Jared Browne, Head of Data Privacy at FEXCO Group

Working Group Members

- Audrey Barrett, Data Protection Officer at SIPTU
- Kevin Higgins, Data Protection Officer at Musgrave Group
- Cliona O'Donovan, QA & Operations Manager at National Office of Clinical Audit

About this Guidance:

The purpose of this guidance is to provide advice on, and examples of how, organisations can practically integrate the principles of data protection by design (DPbyD) into their data protection programmes, and, also, how they can demonstrate the effectiveness of the adopted measures. By so doing, it is hoped that organisations' ability to comply with the accountability principle of Article 5 (2) of the EU General Data Protection Regulation (the 'GDPR') will be enhanced. The paper does not propose to cover the related area of data protection by default.

Article 25 of the GDPR requires the following of data controllers:

"Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects".

Although Article 25 (1) of the GDPR requires that organisations consider DPbyD at the planning stage, and *before* the relevant processing activity begins, it is clear, that in order to be effective, these core principles need to be taken into account at all stages of a processing activity's life-cycle, both before and after the activity is initiated. The relevant European Data Protection Board guidance, *Guidelines 4/2019 on Article 25 Data Protection by Design and Default*, notes: 'Controllers shall implement DPbyD *before* processing, and also *continually* at the time of processing, by regularly reviewing the effectiveness of the chosen measures and safeguards.'

The design stage is critical for incorporating DPbyD into the relevant processing activity, but the demonstration of its efficacy, of whether or not those measures are actually achieving their intended goal, is something which can only be assessed at the post-design stage. As such this guidance paper looks at DPbyD principles in a more-inclusive manner, tracing the progress of these principles across the wider life-cycle of a processing activity to illustrate how their effectiveness can be demonstrated.

Data Protection by Design: Making it Effective

a. Pro-active and On-going Risk Management:

An accurate and up-to-date knowledge of the data protection risks within an organisation is an essential tool for the implementation and maintenance of an effective DPbyD framework. A knowledge of risks allows controllers to implement processes that take account of underlying threats and to mitigate them wherever possible. Organisations must first understand their data protection risks *before* they go about designing controls to mitigate those risks. Otherwise, they are building in the dark against threats that have not been fully identified or understood.

It can be difficult to assess and identify data protection risks, and although risk thinking should always be forward looking, a prudent first step is to highlight data protection issues and incidents that have occurred in the past. Risks cause incidents, and if the underlying risks that caused previous incidents have not been completely mitigated or avoided, they should be included as part of a current risk assessment.

Once risks have been identified, it is recommended that data protection risks are recorded in a risk register. This risk register should record a description of each risk as well as information as to the likelihood of the risk causing an incident, and the impact of an incident resulting from this risk. Each record should also indicate a business role that is responsible for the risk.

Risks can also be identified as the result of a data protection impact assessment (DPIA). It would be counterproductive to conduct a full DPIA for every change conducted within an organisation, and as such it is essential to have a process in place that identifies if a DPIA is required or not. As a baseline it is recommended that if a project or change involves a system or process that handles personal data, the organisation should consider whether the change or project falls within the scope of one of the activities that have been expressly identified by the Data Protection Commission as requiring a DPIA:

https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments.

It should be noted, also, that when assessing risks as part of any DPIA process, the focal point must be the data subject, not the organisation. In practical terms, this means that the relevant risks are those which have the potential to impact *the rights and freedoms of data subjects*, and not general risks to the organisation itself. A DPIA which analyses business risk but fails to talk about data subjects is not a DPIA; it is a misplaced exercise in corporate risk management.

In complex corporate structures, with many business units falling within a wider group-type organisation, consideration should also be given to how data protection risk is built into enterprise risk-management activities. In particular, where varying business areas conduct their own risk assessments, a standard approach to managing data protection risk should be mandated.

b. Establishing KPIs:

A key part of demonstrating the effectiveness of any DPbyD programme, is the establishment of key performance indicators (KPIs). KPIs allow data controllers to understand where they meet/fall short of expected standards, and provide easily-digestible metrics for management reporting. KPIs should track core components of data protection compliance. The following are examples of relevant KPIs in the context of DPbyD:

- DSAR performance: the volume of requests received and the percentage completed within statutory timeframes.
- Data breaches/security incidents: the number of qualifying incidents, how many were near misses and how many were actual data breaches?
- Data breach notifications: whether or not breach notifications were made on time to the relevant regulator, and, where applicable that data subjects were notified in a timely manner.
- Training: what is the % training completion rate for data protection training?
- Data Protection impact Assessments (DPIAs): assessing the timely completion of DPIAs and how many were completed prior to the beginning of the relevant processing activity.
- Audit: the results of any internal audits.
- Complaints: the number of complaints relating to data protection matters.
- Data retention/destruction: that records are being destroyed according to formal schedules in a timely manner.

c. Establishing Data Protection Checkpoints:

In order to create, permanent controls, that ensure that DPbyD principles are implemented effectively, the data protection function should strive to create data protection checkpoints throughout the organisation. In real terms, these are often pre-existing frameworks/procedural documents/questionnaires through which an organisation's daily operational work already flows. If data protection considerations can be effectively woven into these work practices, then the data protection function knows that data protection considerations will be given due attention when they need to be, early, and at the various key junctures in a business's activities.

Managing to incorporate data protection in this way is not only a successful compliance measure, but it is also represents a much more efficient use of time and resources, compared to the data protection function trying to be the ever-present watchdog, monitoring activity, as it were, over the shoulders of employees. Once these data protection checkpoints are in place, data protection compliance can begin to take place, even when the data protection function is not actively monitoring the process. The following are some operational examples of effective data protection checkpoints. There are many other ways in which data protection principles can be embedded into an organisation; the key thing is to search for existing processes that can readily double-up as a data protection checkpoint.

- **Procurement Questionnaires:** Procurement processes are a key point at which data protection requirements can begin the journey of seeping into all levels of an organisation's structures. This is an opportunity to run the rule over third-party suppliers *before* they have contracted with your organisation and *before* they have begun to process *your* personal data. Targeted, broad questions, included in the procurement questionnaire, act like an early warning system to alert you to potential downstream data protection risks and issues that might arise from using the provider in question. For instance, if the contract involves the processing of special category personal data, you might want to ask if the third-party has appointed a data protection officer, has up-to-date data protection and privacy policies, and maintains documentation on various technical and organisation measures. Although it is extremely useful to gain an early understanding of a new third-party at the procurement stage, any analysis conducted at this point, should not replace the more extensive data protection due diligence that will take place at the contract negotiation stage.

- **Project Management Frameworks:** A vital place for the inclusion of data protection principles is within the formal project management documentation that organisations adopt. Project managers, charged as they are with ensuring that all key requirements get documented and costed at the earliest stage of projects, can be hugely effective gatekeepers for the data protection cause. For example, an organisation's project charter template should have a standing section on data protection, acting as a reminder for project stakeholders to consider the implications of processing personal data and how the relevant project might create risks for that data. This analysis can then, potentially, lead into the domain of data protection impact assessments, and allow the data protection function, together with the business, to assess data protection risk before the project begins. Operationally, the outcomes of the data protection impact assessment can then inform the course of the project and any work that might flow from it.

- **Software Development Frameworks:** From the perspective of enshrining data protection into the development of technologies, it is imperative that it be built into any software development frameworks used by an organisation. For instance, if AGILE is the chosen software development methodology, then data protection should form a

part of the various iterations of a software development project, and be considered at every stage of the software's evolution. Practically, one of the most effective ways of achieving this is to have a standing reminder about data protection included in whichever issue and project tracking software an organisation uses. This means that every ticket, whether it is newly created, or is being amended, will have to take account of the data protection implications of the software development work at hand.

d. Monitoring Customer Complaints for Data Protection Trends:

Organisations should analyse complaints at regular intervals to detect signs of any weaknesses in their data protection programme. Complaints, although often relating to other customer matters, may also shed light on data protection vulnerabilities that would otherwise not come to light.

If the organisation operates a complaint monitoring system, then data protection should be a defined complaint category and should include sub-categories such as 'data breach', 'lack of transparency' or, perhaps, 'subject access requests mishandled'.

Additionally, where a non-data protection function, such as a customer service manager, is responsible for monitoring complaints, notification protocols should be put in place to ensure that matters relating to data breaches are communicated without undue delay to the data protection function.
Complaints, including data protection complaints, should also be categorised as minor, moderate, serious. However, it should be borne in mind that a high volume of accumulative minor data protection complaints in a particular category should lead to that complaint category being deemed moderate or serious. Finally, root cause analysis of data protection complaints should be conducted and used to drive improvements in organisations' DPbyD programme.

e. First Line Effectiveness: Building an Internal Data Protection Network:

It is not just systems that we need to consider when we look at data protection by design, we also need to consider the people within the organisation and how they are trained and managed. It is often the case that employees perceive data protection as being solely within the bailiwick of the data protection officer or the IT Security Team. In terms of operational reality, however, it is the responsibility of every employee to ensure appropriate protection is provided for personal data on a day-to-day basis.

Similar to standard approaches to health and safety, organisations need to build a culture of data protection awareness. While designated data protection staff have specific, formal obligations, everyone needs to be aware of their obligations to minimise risks to data. A data

protection culture is built on both sound technical processes and people's everyday behaviours.

One of the most effective ways to achieve a culture of data protection is by embedding the concept of data protection into the design of an employee's journey within the company. This begins with their initial induction, which should include training on a company's and its employees' responsibilities in relation to the personal data that is collected and processed.

Yearly refresher training should then be provided to ensure that employees are reminded both of their responsibilities and the internal data protection policies and procedures.

Aside from training programmes, organisations should use a wide variety of means to regularly re-inforce the importance of data protection whether through newsletters, company intranet forums and any other company-wide communication channels that exist. A multi-channel approach necessarily increases the likelihood of the message being received and understood.
If a business is intent on making data protection a priority, it should also consider incorporating a data protection metric into employee performance assessments, thereby connecting data protection with a tangible consequence.
While all employees should be aware of who within the company is responsible for data protection, in larger organisations there can often be a disconnect between different levels of the organisation and different departments. As such we recommend that larger organisations consider appointing data protection champions at a regional (for multi-national companies) or departmental level. These champions would receive more extensive training from the data protection function and would have regular meetings with him/her to provide updates about data protection developments within their area of responsibility.

The responsibilities of a data protection champion will vary according to region, department and organisation, but they should always include being an accessible point of contact for data protection matters, being a knowledge holder for data protection processes within their area, and being an advocate for data protection best practice.

Similarly, careful thought should be given to who is best-suited to fulfil the role of data protection champion, both in terms of their aptitude and their seniority. In terms of aptitude, although there cannot be a prescriptive rule to determine uniform suitability, in general terms, any staff member whose role requires an exact process-driven mentality together with strong attention to detail will have the right mind set to ensure day-to-day observance of data protection compliance. As regards, seniority, the chosen person should have enough authority within their business unit to be heard, and heeded, when advocating for data protection amongst colleagues.

In this way motivated, knowledgeable data protection champions can become the first line of any data protection programme, and help to ensure that data protection is being effectively implemented throughout an organisation.

f. Second Line Effectiveness:

Much like any compliance programme, the data protection function should establish a monitoring and audit programme to assess first-line effectiveness. While not as in-depth as a third line audit, second line data protection audits should provide on-going comfort to management that key data protection obligations are being met day-to-day.

To be effective these audits should require verification of compliance from the first line, whether it is evidence of consent being given for marketing activities, or of transparency notices being included in Terms and Conditions.
At least annually second line data protection audits should be completed and include an assessment of:

- Adequacy of data protection policies, procedures and guidelines;
- Individual's awareness of their obligations and understanding of policies and procedures; and
- Compliance with policies and procedures within various business areas.

`

g. Third Line Effectiveness: Audit:

A regular and thorough audit of data protection compliance is an essential part of an effective data protection programme. An audit offers the opportunity not only to monitor compliance with existing policies and procedures, but to identify any data or processes that have yet to be accounted for.
It is recommended that a data protection audit should be divided into a technical data protection audit and a business process data protection audit.

I. Technical Data Protection Audit

A technical data protection audit focuses on the technical measures that are put in place to ensure that personal data processed by an organisation is protected. This part of the audit will involve extensive engagement from the Technology/IT department.

Each technical system should be audited for both the presence and protection of personal data. It is easy to assume that a system not directly related to customers or employees does not contain personal data, but these assumptions need to be verified.

Important questions to consider when doing a technical data protection audit of a system are:

- What personal data is stored on the system?
- Is the personal data encrypted at rest and in transit? If so, what level of encryption is applied?
- Is the relevant personal data subject to appropriate data classification?
- Where is the physical storage for the system located and how is it protected?
- How is the system accessed? (i.e. on-site-only access, or is remote access available?)
- How is individual user-access identified and controlled?
- What levels of access rights exist within the system (i.e. full access for all users, access by job role, individual access rights)
- Are backups kept of this system?
- What retention periods are in place and are they automated?
- How many people have privileged access to this system?
- What vulnerabilities, if any, have been identified for this system?

The above questions can serve as a basis for a thorough assessment of each system to ensure that personal data is kept safe and secure and accessed only by people within the organisation with a legitimate business reason for doing so.

II. Business Process Data Protection Audit

This aspect of a data protection audit deals both with the processes that the organisation has in place to handle personal data and the people who handle that data. It is recommended that separate audits be conducted for each business function, and that those participating in the audit are the ones with the greatest knowledge of the day-to-day functioning of that business function.

As part of an audit interview, the records of processing should be reviewed to identify and confirm all personal data currently being processed within the department.

Important questions to consider when doing a business process data protection audit are:

- Has the department processed a new type of personal data, or processed personal data in a new way, since the last audit, that is not reflected in the records of processing?
- Has the department engaged any new third parties to process personal data since the last audit, and if so was the contract reviewed by the data protection function?
- Can an example be provided of a data incident within the department since the last audit?
    - How was the data incident dealt with within the department and was it reported to the data protection function?
    - If the data incident was not reported, on what basis was this decision made?
    - Does the business area clearly understand data breach notification requirements?
    - Does the business area display an acceptable understanding of core data protection policies and procedures?
    - Do the participants have any concerns about personal data processes within the department?
    - Do the participants feel that proper supports are provided to correctly apply data protection processes in the department?

While the above questions will help the organisation identify any unaccounted for changes or oversights, the individual conducting the audit, if possible, should be in a position to query the day-to-day running of the business function, with an aim to identifying any vulnerabilities or gaps.

III. Audit results

A data protection audit should result in a full report detailing the result of all investigations. The report should detail levels of compliance within each business function as a whole, as well as any specific concerns identified. This report should be delivered to the highest levels of management within the organisation, along with any recommendations from the data protection function.

Any recommendations given should form part of the next audit, identifying whether the recommendations were acted upon, to what extent they were acted upon, the business reason for the level of action and how effective the actions have been.

h. Analysing Data Breaches:

Although analysing and documenting data breaches is clearly a requirement under Article 33 (5) of the GDPR, in the spirit of 'never wasting a good crisis' all data breaches, whether significant or minor, should be also analysed with a view to improving organisational and technical measures. A breach, by its very nature, reveals a weakness in an organisation's controls, and, as such, provides a real-world opportunity to take a snapshot of the effectiveness of any DPbyD programme. The following steps are advised in order to gain actionable insights from data breaches:

- In general terms, utilise the crisis opportunity to reshape your DPbyD programme.
- Consider the severity of incidents to prioritise importance and to understand the extent to which organisational and technical measures need to be amended.
- Implement a lessons-learned exercise immediately after handling a data breach. The exercise should include a description of the event, an assessment of its impact, an analysis of the root cause, a summary of the remedial steps required, and an assignment of actions to key stakeholders. A breach that is not learned from is a breach that will be repeated, so it is vital that any required improvements to technical and organisational measures receive management approval in the immediate aftermath of the breach when the issue(s) are still receiving due attention.
- Aside from analysing one-off breaches, regular reviews of data breach logs should be conducted to identify any trends that may indicate underlying, systemic weaknesses in your control environment.
- Update any relevant systems and processes based on the outcome of any breach analysis.

i. Training:

Training is a key organisational measure and the primary way in which the data protection message is conveyed to all staff. The below steps will assist organisations in using training as an effective tool for practically integrating DPbyD into everyday operations.

- Assess the Organisation's Needs

  Understanding the business model is critical to developing a training plan that meets the organisation's data protection training needs. A documented assessment should include reference to the nature and scope of the business model, the existence of different geographical locations, the number and type of departments within the organisation, and the data processing activities carried out by the organisation.

  The business model assessment should seek to identify high-risk departments and activities to ensure training is scheduled on a priority basis.

- Conduct a Training Needs Analysis

  Analysis of the business model assessment should inform the organisation on what it seeks to achieve from its training plan. Based on this, the organisation must determine to what extent it intends to train employees on data protection.

  While it is recommended that an organisation should develop uniform data protection training, providing a baseline standard for all staff, this, where possible should be complemented with bespoke training that considers the differing needs of audiences. For example, information technology and finance functions will likely have specific needs around data security, while sales or marketing departments may require more focus on topics such as consent and compliant advertising techniques.

  The geographical location of business units will also determine the training agenda, and in some cases may lead to the requirement for data protection training on regulations other than the GDPR. It may also identify a need for training to be provided in multiple languages.

  Training should also be integrated with risk management and give consideration to identified risks which can be prioritised when designing the relevant material.

- Assess the effectiveness of training

  Review pass and fail rates to assess the effectiveness of the training; and pay attention to questions that are frequently answered incorrectly – this is an indicator of an area of common confusion where more targeted data protection education is likely required.

- Regularly review training plans

  Review training plans on an annual basis to respond to known risks and areas of concern.

  Additionally, always consider ad hoc learning opportunities, such as data breaches. These are occasions when the root cause of the breach should be identified and then form the basis of the required training.

j. Change Management:

The organisation should have a robust change management methodology in place that deals with any change that evolves or transforms the organisational goals, processes, technologies, and core values. Generally, the objectives of any organisation's change management policy is to successfully implement strategies and methods for effecting change. This policy should have a clear step that triggers the identification of changes that affect or contain personal data. Examples of changes may include:

- The introduction of new technology.
- Changes to existing technologies and/or processes.
- Mergers, acquisitions, or transfer/sale of any assets.
- Change in organisational structure/culture.

Each person in an organisation who handles data needs to be aware of the necessity of GDPR compliance in affecting any new change. Consideration should also be given to the change management methodology being used by an organisation and to what extent this fosters a culture of effective data protection compliance.

Agile methodologies are flexible and embrace changes from the offset of a project. Through a process of iteration, that requires checkpoints at defined stages, the impact to personal data can be repeatedly assessed. A more traditional Waterfall Model adopts a more linear, sequential approach to change management.

Embedding DPbyD into the Waterfall Model

The Waterfall Model generally adopts a linear, sequential series of phases, where each phase depends on the deliverables of the previous one to determine the input for the next phase. This model tends to be among the less iterative and flexible approaches, as progress flows in largely one direction ("downwards" like a waterfall) through the phases of conception, initiation, analysis, design, construction, testing, deployment, and maintenance.

It would be recommended that the requirement of completing a Data Protection Impact Assessment (DPIA) be conducted during the first two phases to ensure that DPbyD is embedded into projects at the outset. Projects involving personal data should have strong change-management controls in place, and in effect not advance to the next phase until data protection requirements are approved.

Embedding DPbyD into the Agile Model

The Agile method involves discovering requirements and developing solutions through the collaborative effort of self-organising and cross-functional teams and their customer(s)/end user(s). It advocates adaptive planning, evolutionary development, early delivery, and continual improvement, and it encourages flexible responses to change. The Agile method is often implemented to organise teams in responding to the unpredictability of a change. This methodology uses numerous incremental work cycles to produce a constantly progressing change output.

It would be recommended that data protection impact assessments (DPIAs) maintain this fast-paced and evolving approach and are revisited, and re-interpreted, at key junctures throughout the cycle. Conventional DPIAs fit better with infrequently updated projects; while, on the contrary, any changes created using the Agile method require a constantly evolving DPIA. A data protection champion should be assigned to Agile projects, so that a focus can be kept on personal data throughout the various iterations.

Establishing a simple system of recognising, communicating and recording impacts to personal data will, ultimately, help organisations to ensure that the principles of DPbyD are incorporated into any change releases.

Appendix 1

Checklists for Incorporating Data Protection by Design Principles

DSAR considerations when designing systems.

- Can information required by Article 13/14 of the GDPR be provided to the data subject in a timely manner?
- Can personal data be identified on receipt of a DSAR?
- Can personal data be extracted to comply with a DSAR?
- Can personal data be deleted if necessary?
- Will other data subjects' rights and freedoms be safeguarded during the process?

Applying Data Protection by Design to the Core Principles of Data Protection

1. **Lawful, Fair and Transparent**
   - How are data subjects made aware of the processing?
   - Has the nature of the processing been made transparently obvious to the data subjects?
   - Has the legal basis for processing the information been determined?
   - Is consent required to process the personal data?
     - Can you prove consent was given, and when?
     - How will you maintain records of consent?
     - Is the request for consent presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language?
     - Is there a process which allows the data subject to withdraw consent?
   - Is data being transferred to a third country or international organisation outside the EU? If yes, what legal mechanisms and/or supplementary measures are being relied upon?
     - Understanding it from the perspective of the customer, is there anything in the processing activity that could be construed to be unfair?
2. **Purpose Limitation**
   - Is personal data collected for specific, explicit purposes?
   - Has it been clearly established if there is one or multiple purposes in scope?
   - Are there procedures in place to mitigate against the risk of scope creep?

3. **Data Minimisation**
    - Can you justify why each type of personal data is collected?
    - Is the logic for collecting the data clearly guided by the underlying purpose?
    - Can you ensure that data will not be duplicated across systems or platforms?
4. **Accurate and Up to Date**
    - Is the data accurate?
    - Where necessary, is it kept up to date?
    - If the data becomes inaccurate, is it rectified or erased without undue delay?
    - Are there system controls in place to identify the presence of inaccurate data?
5. **Retained Only for as Long as Necessary**
    - Is there an agreed retention period which permits identification of data subjects for no longer than is necessary for the purposes of processing?
    - Has this the operation of this retention period been automated?

ENDS