THE OFFICE OF THE
Data Protection Authority

The Data Protection (Bailiwick of Guernsey) Law, 2017 ("the **Law**")

Data Protection Measures by Design and Default

What is "Data Protection by Design and Default"?

Section 32 of the Law requires data controllers to establish and carry out proportionate technical and organisational measures to effectively comply with the data protection principles, ensure that by default only personal data that is necessary for the purpose is processed and integrate necessary safeguards into their processing to ensure compliance with the Law and safeguard the rights of individuals.

It is therefore a legal obligation on controllers to incorporate and be able to evidence data protection compliance from the outset of any project or process that involves personal data. Examples may be

- Designing and building new IT systems
- Updating existing policies and procedures or writing new ones
- Considering data sharing initiatives
- Collecting any new data

In all such cases, and any others that will or are likely to involve personal data, data protection must be a key consideration at the very first stage of the project. It must also be integral to the events lifecycle.

The concept of 'Data Protection by Design and Default' requires controllers to ensure that the 'default setting' or starting point when considering the processing of personal data

ensures the highest standards of compliance. The aim is for data controllers to embed data protection compliance into any procedures or products that they implement or develop and that involve the processing of personal data.

Data protection compliance should be the baseline for the project and a core component of functionality rather than an add-on once the project has commenced. If the data subject does nothing more than request the service or use the product, their data protection rights should be paramount and routine. For some, this may involve a significant cultural shift and a need to revise internal processes as well as train employees. Such an approach must be led from the top of any organisation and will help to ensure that the personal data of customers and staff alike are protected. In today's digital world, the protection of our data should be important to all of us as consumers. Data Protection by Design and Default is intended to embed a culture of respect for privacy into organisations and recognition that personal data is a valuable asset and should be treated as such.

Previously, it has been good practice to adopt this approach. However, both the General Data Protection Regulation (the GDPR) and the new Data Protection (Bailiwick of Guernsey) Law, 2017 (the Law) make 'Data Protection by Design and Default' a legal requirement from 25 May 2018. There is an expectation that controllers will be able to demonstrate that data protection compliance requirements have been considered at the design and implementation stage of all processing.

It is important to remember that data protection should remain on the agenda throughout the development and implementation phases, not just at the outset. It should also be considered when reviewing existing processes and procedures - this approach does not just apply to "new" products or procedures.

Successful compliance with data protection legislation requires more than a 'checklist' approach. In order to successfully limit the risks (both for businesses and consumers alike), controllers should ensure that privacy is not simply added on as an afterthought, but forms a core part of their approach to doing business.

Implementation is equally important. To that end, 'Data Protection by Design and Default' involves looking at these issues across the entirety of the business and with the active engagement of all relevant stakeholders. Having a policy or procedure is a good starting point, but it needs to be followed in practice by all employees to be effective.

What are the benefits?

The 'Data Protection by Design and Default' approach enables:

- greater transparency and accountability;
- controllers to demonstrate effective and meaningful compliance with the Law;

- data protection issues to be identified and dealt with at an early stage, thereby reducing or eliminating potential risks and remediation costs as the project progresses;
- a "privacy friendly" culture to develop within organisations, which reduces the risk of non-compliance and once in place can run by its own momentum;
- a less intrusive approach to the handling of personal data.

Whilst the Law refers in part to the 'Data Protection by Design and Default' approach as a tool for use in demonstrating compliance, it has further benefits to both businesses and consumers.

Individuals are afforded strengthened rights in relation to their personal data under the Law. The issue of trust and having confidence in those handling our personal data is vital if we are going to be a jurisdiction that embraces the obligations that come with being part of the data economy. Being able to demonstrate that the protection of data is taken seriously within an organisation is not simply helpful in terms of regulatory compliance - it is increasingly seen as a method of building and retaining consumer trust and confidence.

It is also important in terms of protecting the integrity of your supply chain. Controllers have an obligation to ensure that those third party service and product providers with whom they contract as processors have appropriate data protection standards in place. The procurement process should therefore involve full and documented consideration of privacy issues and how the proposed supplier intends to meet those requirements. This means considering privacy not only from the perspective of the product or service being offered, but also in terms of how the supplier will manage any personal data it is processing on behalf of the data controller.

By identifying issues at the outset and keeping them under review, you should be able to identify which suppliers are able to meet the privacy requirements under the Law and work with them to implement any changes to the product or service (or to their operational methods) which might be required.

Adopting the 'Data Protection by Design and Default' approach may involve a cultural and/or organisational shift in terms of adopting new methods of working, input from additional stakeholders within the business, or revisions to existing procedures. Any such changes should be made with the specific needs of the business in mind - there will not be a "one size fits all" method which will work for everyone.

Some examples of situations where the 'Data Protection by Design and Default' approach applies include:

- offering a new product or providing a new service to customers;
- the implementation of a new security/access protocol for an office building or document management system;

- planning a new marketing campaign or using a new marketing platform or database;
- outsourcing administrative functions including HR and email support services to third parties;
- purchasing a new data hosting or data sharing platform; and
- development of a new app for use on mobile devices.

These examples are not exhaustive and are designed simply to provide an indication of the types of situations where the 'by design and default' approach would need to be applied.

What are the privacy issues that we should be considering?

Compliance with the Data Protection Principles is a core requirement of the Law and 'Data Protection by Design and Default' requires that appropriate technical and organisational measures are adopted to achieve that aim. This means considering the Data Protection Principles throughout the design and development of procedures and/or products.

It may be the case that not all of the Principles are relevant or applicable to each situation. The key issue is understanding and mapping the proposed data processing and understanding where the risks may lie and how to address them.

Any steps that you do take should be 'appropriate'. This means that not only are the measures designed to achieve the stated goal, they should also be 'proportionate'. If the risks for data subjects associated with the processing are high, then you will be expected to allocate more time and resource to managing those risks and implementing more rigorous solutions than if the risks have been identified as low.

The legislation refers to both 'technical and organisational' measures when ensuring compliance. In some cases, there may be a technological solution. In others, the response may involve a human element. In most situations, it will be a combination of the two. This may involve training staff, restructuring a team or implementing a new policy. We encourage data controllers to think in the round to ensure the efficacy of the systems and processes being implemented.

For example, an effective solution may not simply involve the IT team putting in place additional access controls. Staff engagement and training will also be required to ensure that such controls are actively managed and not circumvented, either deliberately or in error, by staff members. Staff will better comply with such measures if they understand what they are trying to achieve and the importance of data protection to the organisation. There may also be physical considerations to take into account, such as the location of the servers, access to the premises, security around remote access to the software, use of laptops for remote working, etc.

At the heart of the thought process is the protection of the personal data in your possession - how can the Data Protection Principles be complied with in the context of the product, service or procedure being considered? We encourage controllers to consider these issues with involvement from stakeholders across the business in order to ensure that the 'Data Protection by Design and Default' approach is effective. There are likely to be operational, legal, HR or other issues to consider as part of the design process so it will be important to engage all relevant parties.

We anticipate that controllers will have a range of questions as to whether the steps they have taken are appropriate and/or proportionate. It is inevitable that these assessments will have to be undertaken on a case by case basis, but the Law and the GDPR both give indications as to the broad factors to consider.

These include:

- the nature of the processing;
- the scope of the processing;
- the context of the processing;
- the purposes of the processing;
- the solutions available on the market, what your competitors are doing and what could you be doing?;
- the costs of implementation;
- the risks associated with the processing; and
- the severity of the impact on the rights and freedoms of data subjects.

Ascertaining whether proposed measures are 'appropriate' in the circumstances is a matter of considering the above factors in the context of the business and the risks associated with the processing. That analysis is crucial in determining how to approach 'Data Protection by Design and Default' and the measures to put in place to meet not only those requirements, but the obligations under the Law.

Data Protection Impact Assessments (DPIAs)

Section 44 of the Law requires controllers to carry out an assessment of the impact of the proposed processing operations on the protection of the personal data in their possession where the processing is high risk.

Even if a full DPIA is not required, it is considered good practice for controllers to undertake a risk assessment involving the consideration of the privacy and data protection issues, and this will assist in informing the measures which might be required. It can also be good evidence of compliance with the 'by design' approach required by the Law.

Consider what impact the idea or proposal has from a data protection perspective.

- Can the idea simply be put in place using existing controls and procedures, or does something additional need to be done to safeguard the current and future interests of data subjects?
- Is there a need for additional policies or procedures?
- Will staff training be needed?

Once that risk assessment has been completed and documented, the controller can then look at implementing solutions which are appropriate to deal with the relevant risks. It is also then important to be transparent with data subjects as to what is being done with their data and the risks involved.

Screening questions to determine whether a DPIA is necessary and a suggested DPIA template are available on our website.

Do you have examples of the sorts of measures that may be used?

The nature and type of measures which might be put in place to give effect to 'Data Protection by Design and Default', or which may be of wider benefit in terms of broader compliance with the Law, are necessarily dependent upon the context of the processing and the business itself.

However, some examples of possible measures include:

- Minimising the processing and personal data held – this is already a legal requirement and it is worth remembering that more personal data than you need increases the risk to the organisation with no benefit;
- Involving the data protection officer and all stakeholders within the business in the design process;
- Limiting access rights (both physically in terms of security of premises, access to hard copy files, etc. and digitally by virtue of password protection, "lock down" of files, etc.);
- Reviewing the process by which personal data is handled and/or transferred;
- Transparency in the processing – this is already a legal requirement – but it is worth bearing in mind that explaining the processing fully to data subjects will reduce their concerns and increase trust as well as ensure compliance;
- Allowing the data subject to monitor the processing or to control their personal data through a portal or similar;

- Considering the impact of any proposed international transfers and the mechanisms by which they could be effected – this is already a legal requirement but proper consideration of the best method to safeguard transfers will minimise the risk inherent with transfers; the simplest way is not always the best;
- Anonymising or pseudonymising the data;
- Feedback function to allow the controller to create and review security features
- Having a clear strategy as to what data will be collected, on what basis and for what purpose(s)

When reviewing the measures to adopt, controllers should have reference to their DPIA and ensure that there is a documented record of the considerations that formed the basis of the decisions subsequently made. This will not only aid any future decisions to amend or revise the approach, but will also assist the Office of the Data Protection Commissioner ("ODPC") in terms of demonstrating compliance in the event of enquiry.

Data Protection by Default

This means that privacy is the "starting point" or "default setting". For instance, data controllers should ensure that they are only processing the personal data that is necessary to fulfil a specified purpose. This minimises the data being processed and reduces the risks involved in processing. Any 'privacy' settings on a product or contained within a service should be provided at the maximum level available with that product as a default.

Data controllers should assume that personal data will not be processed (including collected) if there is no clear and lawful need to do so. In the context of a social media profile, for example, the privacy settings should (by default) be set to the highest levels of privacy. It is then up to the individual to decide how much information they share, and importantly, with whom and for what purpose. It is clearly important to ensure that the transparency obligations are complied with to ensure data subjects have all relevant information provided to them to allow them to make informed and personal decisions.

A great starting point is to consider how you as an individual would feel about the processing and the safeguards that are being proposed as part of a product or service. If you yourself would feel uncomfortable about your personal data or that of a loved one being used in that manner, your clients and customers are likely to be concerned too.

The Law requires appropriate technical and organisational measures to be taken to limit, by default:

- the amount of personal data processed
- the extent of its processing
- the period of its storage; and

- its accessibility (in particular ensuring that the data is not made available to an indefinite number of persons without human intervention).

Again, the question as to what amounts to 'appropriate' measures should be considered in the context of the DPIA carried out in respect of the proposed data processing. However, in the context of 'Data Protection by Design and Default', those considerations have a common goal, the minimisation of risk and limiting of the processing to what is necessary to fulfil the purpose. To that extent, it is anticipated that a process which aims to reduce the processing and/or amount of data collected and stored, would be considered to meet the requirements.

Certification/Codes of Conduct

The Law makes provision for the ODPC to recognise certification and codes of conduct as measures of compliance. At present, there are no formally recognised certification standards or codes of conduct that have been approved as "GDPR/Guernsey Law" compliant. However, please refer to our website regularly for updates in this regard.

Guidance and Other Resources

DPIA 1 – Screening Questions

DPIA 2 – DPIA Template

DPIA 3 – Data Protection Principles – areas of risk

UK ICO DPIA Guidance