Introduction

Accountability and 'privacy by des of UK Data Protection Legislation. For the purposes of these guic tection Legislation" refers to all applicable data protection and pri not limited to, the retained EU law version of the General Data Prote 2016/679) (the "UK GDPR"), as it forms part of the law of England and Northern Ireland by virtue of section 3 of the European Union the Data Protection Act 2018, the Privacy and Electronic Communic as amended, and any successor legislation.

These guidance notes have a pa GDPR and the principles set out therein. The UK GDPR in fact refe as 'data protection by design and default' but to keep things simple, guidance notes to use the phrase 'privacy by design'.

An important aspect under thes Protection Impact Assessment, previously known (again, more sim Assessment.

Data Protection Impact Assessme elp to identify and minimise data protection risks. In some cases, t er the Data Protection Legislation and, in other cases, simply good p ur business is processing personal data (and it most likely is), particul "likely to result in a high risk to the rights and freedoms of [data subj conduct a DPIA for new projects and, possibly, when reviewing exis e.

Assessing risk is an important ot least because it is what will determine whether a DPIA is nec e central point, when considering risk, is to examine the likelihood a the impact that the personal data processing in question will have ects. Even before undertaking a DPIA, therefore, whenever a ne is being planned, risk must be considered in order to determine tion and analysis, in the form of a DPIA, is needed.

[1] Article 35(1) UK GDPR.

Part 1. What is a Data Pro sessment?

DPIAs are covered by Article 35 serve as a means to analyse the collection, holding, and processing view to identifying risks posed to individuals and minimising those mphasise *minimising*. You are not necessarily expected to eliminate ensure that you can take steps to mitigate them and that they are jus

The concept of a DPIA is not ne sations carried out Privacy Impact Assessments long before the EU PR) came to be. In some parts of the world, Privacy Impact Assess mandatory requirement before the advent of the EU GDPR in 2018. M assessments were and are in fact more comprehensive than the UK A.

At a minimum, a DPIA must conta

a) a systematic desc d processing operations and the purposes of the pro e applicable, the legitimate interest pursued by the [dat

b) an assessment of roportionality of the processing operations in relatio

c) an assessment of th freedoms of data subjects…; and

d) the measures envis ks, including safeguards, security measures and mec protection of personal data and to demonstrate compl PR] taking into account the rights and legitimate intere other persons concerned.[2]

[2] Article 35(7) UK GDPR.

Part 2. When is a DPIA Re

As noted above, a DPIA must be use personal data in a way that is likely to result in a high risk to in R sets out three types of personal data processing which will always ertaken:

e) any systematic an of personal aspects relating to natural persons wh ed processing, including profiling, and on which decis duce legal effects concerning the natural person or si person;

f) processing on a lar gories of data referred to in Article 9(1), or of personal convictions and offences referred to in Article 10;

g) a systematic monito ble area on a large scale.[3]

Guidance published by the EU's y (now replaced by the European Data Protection Board) provides th may indicate a likelihood of high-risk personal data processing (the g a DPIA):

- Evaluation or scoring;
- Automated decision-makin gnificant effects;
- Systematic monitoring;
- Sensitive data or data of a
- Data processed on a large
- Matching or combining dat
- Data concerning vulnerable
- Innovative use or the appli al or organisational solutions;
- Preventing data subjects fr using a service or contract.

In addition to the criteria set out ab mmissioner's Office ("ICO") has its own list (some parts of which are e), requiring organisations to carry out a DPIA if they intend to:

- use innovative technology y of the criteria from the Article 29 Working Party's criteria, ab
- use profiling or special cate cide on access to services;
- profile individuals on a larg
- process biometric data (in of the criteria from the Article 29 Working Party's criteria, ab
- process genetic data (in f the criteria from the Article 29 Working Party's criteria, ab
- match data or combine dat ces;
- collect personal data from he individual data subject without providing the individual wit "invisible processing");
- track individuals' location o
- profile children or target ma s to them; or
- process data that may end subject's physical health or safety in the event of a security b

As noted above, conducting a DP roject is good practice regardless

[3] Article 35(3) UK GDPR.

of the risks present; however, ev t is not necessary to do so, it is important to remember the accou ping principles set out by the UK GDPR. Demonstrating compliance siness handles personal data, you should keep evidence of the ste the Data Protection Legislation. Therefore, even if a full-size DPIA nding and the reasoning behind it should be documented.

Particularly for small businesses, cessary to conduct a DPIA purely on the basis that only simple, low- ssing will be undertaken; however, at the risk of being repetitive, just echnically required does not mean that it is not still a good idea to car

If there is any doubt as to whethe u should always consult the ICO.

Part 3. Carrying Out a DP

The ICO separates out the DPIA in

a) Identify the need fo
b) Describe the perso
c) Consider consultati
d) Assess the necessi he processing;
e) Identify and assess
f) Identify measures t
g) Sign-off the DPIA a
h) Integrate the outcor ; and
i) Keep things under r

3.1 Who Should Be Involved?

First, however, you should establi lved. If your business has a Data Protection Officer ("DPO"), they t of call. The ICO's guidance on DPIAs states that the DPO should e guidance on some key points:

- Whether or not a DPIA is n
- How the DPIA should be c
- Whether the DPIA should b -house;
- The measures and safegu to mitigate risks identified by the DPIA;
- Whether or not the DPIA ha ctly; and
- The outcome of the DPIA not the proposed personal data processing can take place.

In line with the concluding para e, the DPO's advice should be documented. In particular, if yo that advice, your reasons and justifications for that decision shou

The DPO should also be respons ongoing performance of the DPIA and they must be able to do so any conflicts with other assigned duties.

Others who should be involved in t e:

- Staff involved with informat
- Any third-party data proces osed processing; and
- Other relevant experts and

3.2 Describing the Personal Data

This stage of the DPIA should giv the personal data involved in the proposed project; how it will be co ed, how it will be stored. Consider the following key points:

a) The nature of the … how the personal data will be collected, stored, a… who will have access to the data, whether or not it … er third-party processors will be involved, how long … what security measures will be in place to protect it, …gies are involved, whether novel types of processin… which of the screening criteria covered above have …isks.

b) The scope of the p… nature of the personal data, the volume and variety …ta will be (e.g. special category personal data), the …duration of processing, how many data subjects will be …aphical area covered.

c) The context of the …actors such as the source of the data, how you are …duals involved, how much control those individuals w…nal data, whether or not they are likely to expect th…considering, whether any of the individuals are likel… vulnerable people, any previous experience you hav…ssing proposed, relevant advances in technology or s…es, any related issues of public concern, and whet…mply with any codes of practice, codes of conduct (a…roved) or certification schemes.

d) The purpose of the … your legitimate interests (if this is your lawful basis fo…ed outcome for the individual data subjects involved, a…s.

3.3 Involving Individual Data Su…

Unless you have a good reas… ICO recommends seeking (and documenting) the views of individu…ves as part of a DPIA. Should you decide not to, this decision itself sh…

It may, for example, be undesirab… data subjects during your DPIA if commercially confidential inform…omised or if security might be undermined.[4] It may also simply be …racticable.

In many cases, your proposed pro…als with whom you already have a relationship of some kind – your c… Situations like this in particular are those in which it might be difficult … with affected individuals would be disproportionate or impractical. T… should consider a suitably user-friendly means of consulting them.

If, on the other hand, the data sub…ject are not already known to you, a more general approach will be r… research targeted at the relevant demographic.

It is important to remember that w… what your customers, employees, or other individuals want. What se… you may seem like an intrusive or otherwise undesirable use of pers…re not necessarily bound to abide by feedback received from individ… that you document your decision-making process fully, including …stification for disregarding such unfavourable views. This may als…te lawful basis for using personal data and touch on various data su…right to object to processing. Even

[4] Article 35(9) UK GDPR.

if you do decide to go against the r individuals, tread carefully.

3.4 Assessing Necessity and Pr

An important principle of the UK ion. In short, only gather and use what you need. By focusing on nality, you benefit both the data subject and your own business. D ghts, and freedoms are protected because you do not have an exces a, and your interests are protected because you are exposed to less event that anything goes wrong in the future.

As part of the DPIA, therefore, it whether your planned collection, holding, and processing of person s the stated purpose and whether there are any reasonable alternati

Furthermore, the Article 29 Wor highlights the following points to consider under the heading of n ality. Many of these points relate closely to the UK GDPR's core pri urse, you should always comply):

- Your proposed specified, urpose(s) for processing personal data;
- Your proposed lawful basis ;
- Limiting personal data to th evant, and necessary;
- Only holding personal data it for your purpose(s).

It is also very important to conside rights of individual data subjects:

- Providing the required infor
- Ensuring that data subject of access and (where applicable) data portability;
- Enabling data subjects to e tification and erasure;
- Supporting data subjects' r trict processing;
- Keeping your use of data p cessing on your behalf) compliant with the Data Protection Le
- Safeguarding international personal data.

3.5 Assessing Risk

A risk assessment is, in many wa A. Risks should be both identified and assessed in terms of likeliho ning that stands to have a severe impact but that has a remote ch ents less risk in real terms than something with a moderate impa of occurring. Similarly, something that would result in only minor ha ly to occur could be considered a higher risk.

Some of the factors to consider wh e:

- Individual data subjects be eir rights;
- Individual data subjects be ain services or opportunities;
- Individual data subjects los sonal data;
- Discrimination;
- Identity theft;
- Fraud;
- Financial loss;

- Damage to reputation;
- Physical harm;
- Loss of confidentiality;
- The re-identification of data ymised (e.g. through combination with other available data);
- Other significant social or e

Your risk assessment should also security risks, including the likely sources of such risks and their po be appropriate to consider other compliance and legal risks, such er privacy legislation such as the Privacy and Electronic Communica

In addition, while not necessarily subjects' rights or even your own obligations as a data controller un egislation, it may also be useful to include organisational and comme er be forgotten that, in addition to the potential fines for non-compli R, reputational damage stemming from a data protection failure can b

Having identified risks, your DPIA hich those risks can be mitigated.

3.6 Mitigating Risks

Every problem, as the saying go this is equally the case when it comes to most data protection risk The entire purpose of the DPIA is to make you stop and think about pposing is safe and lawful, both for data subjects and for yourself.

For each risk identified, dependin d severity, a solution or at least a means of mitigating it should be i s, these solutions will be simple – even obvious – such as providing really should be standard practice for you by now!). In other cases, stic and require a substantial re-thinking of the entire project. Whe mitigated or otherwise), responses to those risks in the event that they ould be considered.

You may, for example, decide to ories of personal data you were planning to collect, or to reduce t some risks might be mitigated by using technological solutions no . In other cases, organisational changes such as staff training, edures, new or amended privacy notices, or the implementation of agreements with third-parties may solve the potential issues.

What is important is that each risk in turn, and the temptation to skip over any should be avoided. In e ase of weighing up the costs and benefits. You are not expected to gation is key, and you must decide (and, as always, document) wheth risk is proportionate, appropriate, and justifiable.

3.7 Wrapping Up

Having considered the solutions to earlier, your DPIA should conclude with what essentially amounts to t how each risk identified will be addressed, and how that solution If some level of risk remains, it is important that this is also noted.

At this point, it is also importan nything highlighted by the DPIA

requires you to consult with the IC a high risk that cannot be solved, even if you plan to continue and a st consult the ICO, as required by the UK GDPR.[5]

If you have a DPO, they should b throughout. Most importantly, they should also be involved in the sign of the DPO on all aspects of your DPIA is essential and if you opt, fo w their advice, this decision must be documented.

[5] Article 36(1) UK GDPR.

Part 4. What's Next?

Once your DPIA has been comp nd the ICO consulted if required, implementation can begin. This d the DPIA process, however. The outcomes of your DPIA should b roject plans and then monitored throughout the project itself. The D purpose if it is simply shelved and forgotten once it is signed off.

It will be important, as your projec that the solutions to risk identified in the DPIA are working as intend e mitigated as expected. It is also essential to continually review th (or internal) factors may change risks, in some cases increasing th tant to remember that the DPIA is not a static process or a one-off e plex the project, the more you will need to maintain a keen awarene d the effectiveness of your chosen solutions. Moreover, the Article 29 also recommends reviewing your DPIAs every three years. Combine ction audits across your business, this good practice can help t ata collection and use remains proportionate, reasonable, and la nnical and organisational security measures are still up to the task o .

One of the core benefits to your b th the Data Protection Legislation (and particularly the well-publicise ou are transparent about your use of personal data and proactive in exercise of their legal rights, data subjects will be more comfortable data to you. Consequently, it can be beneficial to publish DPIAs. T have to be a full version of the DPIA – not least since such docu commercially sensitive confidential or proprietary information – but a e is no mandatory requirement to publish DPIA, and certainly the pra among public organisations than it is among SMEs, but it is neverthe he transparency and trust benefits of doing so.