GemTALK#2 – Questions and Answers

QUESTION 1

Regarding Privacy Notices, are you aware of good examples that are aimed at children? (i.e. intended to be read/watched by under 18s without a parent present to help them understand it)?

Many creative methods can be used. For example, in the context of connected toys, some organisations have used videos to explain to children how their personal data is used. Apple and Lego have clear privacy policies and many interfaces aimed at children. The best example is if you search in Google for "Lego, Legal Notice", you will find Lego's Privacy Policy, which is made clear and accessible for children.

QUESTION 2

How do you address sensitive information that is going external i.e. info sent over email such as passport information?

Encryption could be used to send personal data externally. Alternatively, considering using secure file sharing providers such as Huddle or FileCloud, which are good secure cloud storage and sharing providers.

QUESTION 3

Are there examples of when NOT to conduct a DPIA? Is there a list published by the ICO on this?

There is no such list, as published by the ICO. However, generally – when there is no high risk to data subjects from a new process that doesn't present a high risk to data subjects. As examples, we suggest that you don't need a DPIA for including, for example: switching to a new cloud service provider for B2B data, switching to a new mailing list provider for B2B data, and installing a new firewall.

QUESTION 4

How do we operationalise PbD in already existing Technologies (especially customized applications, COTS), Systems and Processes of organizations?

This depends on the technologies, processes and systems. In general, encryption can be added retrospectively to data at rest or in transit, if not already used. Alternatively, privacy notices and interfaces can be customised to increase transparency in relation to the processing.

QUESTION 5

If you have identified a legal basis for a process as being legitimate interests, and have carried out he necessary LIA to confirm that this is appropriate, would you consider that there should always be a risk on the PIA that you may not have a legitimate interest?

Yes – this will generally be a risk you should consider. As part of the DPIA, you should consider which legal basis you are relying upon, including legitimate interests. As part of any legitimate interest assessment, you should then consider whether;

1. the interest is necessary for your business process;
2. using the personal data in such a way will generally be within the reasonable expectations of data subjects.

QUESTION 6

Are there any requirements unique to the UK regarding DPIAs (vs other EU countries)?

Yes – there are slight differences between some countries. In the UK, the ICO requires a DPIA to be conducted in the following situations:

- Processing involving the use of new technologies, or the novel application of existing technologies (including AI), when applied with any other criterion;
- Processing involves making decisions about an individual's access to a product, service, opportunity or benefit which are based to any extent on automated decision-making (including profiling);
- Processing involves the processing of special-category data;
- Processing involves any profiling of individuals on a large scale;
- Processing operations involve biometric data for the purpose of uniquely identifying an individual, when combined with any other criterion;
- Processing operation(s) involve genetic data when combined with any other criterion;
- Processing involves processing of genetic data, when combined with any other criterion;
- Processing involves combining, comparing or matching personal data obtained from multiple sources;
- Processing involves processing data that has not been obtained direct from the data subject in circumstances where the controller/ when the controller considers that the provision of such information proves impossible or would involve a disproportionate effort, when combined with any other criterion;
- Processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment, when combined with any other criterion;
- The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children;
- Processing that is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals.

Further guidance from the ICO can be found here.

QUESTION 7

Do I need to do a DPIA for each new system I deploy, such as an HR or CRM system?

You will need to conduct a DPIA when there is a high risk to data subjects. As part of this, you should consider the scope of the processing – for example, do you have a lot of employees – hundreds or thousands? Will you collect sensitive data – such as health or criminal data – about them, and store it in such databases or systems? If so, a DPIA may be required.

QUESTION 8

Is the data controller or processor responsible for PbD?

Both are responsible for compliance with Privacy by Design, as a core principle under the GDPR. Fines can be issued to both sets of organisations for non-compliance with this principle.

QUESTION 9

Have any official guidelines been issued in undertaking PbD or DPIAs?

Yes – several have been issued from supervisory authorities in the EU and EEA, such as ENISA, the Norwegian Data Protection Authority and the French CNIL, on Privacy by Design. Additionally, several other European data protection authorities have published DPIA lists, as approved by the European Data Protection Board, which outline where they will require DPIAs to be conducted.

GLOSSARY

GDPR – General Data Protection REgulation
PbD – Privacy by Design
DPIAS Data Protection Impact Assessments
ICO – Information Commission Office
PIA – Privacy Impact Assessment
LIA - Legitimate Interest Assessment