GDPR Interview

https://www.knowist.ac

The following is a collection of sample questions demonstrating the level of knowledge concerning GDPR we will be expecting during our interviews.

- o -

What is the GDPR?

GDPR is the General Data Protection Regulation, otherwise known as (EU) 2016/679.

It is a ground-breaking set of regulations relating to data privacy rights for citizens of the European Union. The GDPR came into force mid-2018.

Even though before that there were some data privacy regulations in European countries, it could be said that previously matters were most arranged to the benefit of large corporations.

In contrast, now with GDPR in force, matters are arranged strongly in favour of citizens and their privacy rights. Significant obligations are placed on corporations that mandate how they must respect citizens' data privacy and the steps organizations need to take to protect access and dissemination of citizens' personal data.

What is the different between a data controller and a data processor?

To quote from the GDPR (Art. 4) - https://gdpr-info.eu/art-4-gdpr/ :

> *'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;*
>
> ***'controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing of personal data;** where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;*
>
> ***'processor'** means a natural or legal person, public authority, agency or other body which processes personal data **on behalf of** the controller;*

What is a DPO?

A DPO is a Data Protection Officer. Art 37 of the GDPR outlines the role of the DPO in the larger picture - https://gdpr-info.eu/art-37-gdpr/

In summary, these are the specialists within an organization who provide oversight and guidance to the other departments on how the GDPR is to be implemented within that organization.

What are the other actors in the GDPR privacy model?

The individual is known as a data subject (the personal data relates to this person). The data subject is the main beneficiary of GDPR. The data subject has rights under the GDPR (whereas the data controller has obligations).

Each country that implements the GDPR needs its own Data Regulator, which is the regulatory authority for that country.

The European Data Protection Supervisor (EDPS) is a EU-wide organization that oversees GDPR across all the countries and plays a coordination role.

Finally the European Data Protection Board (EDPB) is there to facilitate discussion and decision making between the supervisor and each country's Data Regulator (all of which are members).

What is a SAR?

A Subject Access Request (SAR) is a request from a data subject (an individual) to a data controller (an organization) for information about the data the latter holds on the former. There are strict rules in place as to how a data controller needs to respond to a SAR and how long they have.

Can you give a synopsis of the rights that an individual has under the GDPR.

Nicely summarised here:

- https://dataprotection.ie/en/individuals/rights-individuals-under-general-data-protection-regulation

Can you give a synopsis of the obligations organizations have under the GDPR.

Nicely summarised here:

- https://dataprotection.ie/en/organisations/know-your-obligations

What special categories of personal data?

Art 9 of the GDPR - https://gdpr-info.eu/art-9-gdpr/ - outlines a list of categories of personal data for which organizations must implement enhance protection.

It starts with the following statement:

> *"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."*

What is consent and what are the GDPR rules surrounding it?

A data controller must have a valid reason for storing and processing a data subject's private data. Consent is one of these reasons. Consent is where the data controller has clearly requested consent from the data subject to carry out some action and the data subject has agreed.

It is very important to realise there are other reasons (beyond consent) that also allow the valid processing of personal data. See the definition of the "consent" term here for more details:

- https://dataprotection.ie/en/individuals/know-your-rights/definition-key-terms

How difficult is it for an organization to implement GDPR?

For organizations to correctly implement data privacy is like when recycling came in – a big of work at the beginning ("where do I put the extra green bin?"), a bit of education ("what things do I put in the green bin?") but after a while, it becomes second nature and nowadays we would never think of not having recycling.

At the beginning, data privacy does mean some changes to an organization's business practices and computing systems (those "consent" confirmations needed when we visit a website) and staff need to be educated in what GDPR is and how to implement it, but very likely over time it will not be that onerous.

What is the Adequacy Decision?

From the EU website:

- https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

> *"The European Commission has the power to determine, on the basis of article 45 of Regulation (EU) 2016/679 [note: GDPR] whether a country outside the EU offers an adequate level of data protection."*

A country outside the EU and EEA which has been granted an Adequacy Decision has more to process EU citizens' personal data to compared to a third country without one. There is a discussion here:

- https://www.linkedin.com/pulse/gdpr-after-deal-brexit-easier-send-eu-personal-data-o-tuathail/

Give me an example of an Adequacy decision

As the European Union creates new trade agreements with other countries and other trading blocs around the world, the Adequacy Decision will need to be agreed.

One example is the recent EU-Japan trade agreement. This is the announcement of the related Adequacy Agreement:

- http://europa.eu/rapid/press-release_IP-19-421_en.htm

Tell me about GDPR for European countries outside the European Union?

The EEA – European Economic Area – is a grouping of European countries interested in close cooperation at an economic level. This diagram shows the arrangements of European states and groupings:

- https://en.wikipedia.org/wiki/File:Supranational_European_Bodies-en.svg

We see that the EEA has as members all the members of the European Union and three of the four members of EFTA. So Iceland, Norway and Liechtenstein are members of the EEA, whereas Switzerland is not.

GDPR has been incorporated into the EEA Agreement. So GDPR does apply in Iceland, Norway and Liechtenstein. See here for details:

- https://www.efta.int/EEA/news/General-Data-Protection-Regulation-incorporated-EEA-Agreement-509291

What about GDPR and Switzerland?

Switzerland is not part the EEA so GDPR does not directly apply in Switzerland. Switzerland does indeed have strong data protection regulation, but it is similar to rather than the same as GDPR. It is overseen by the Swiss Federal Data Protection and Information Commissioner:

- https://www.edoeb.admin.ch/edoeb/en/home.html

A more detailed look at data privacy in Switzerland is here (to read online just click on chapter names below "chapter content"):

- https://iclg.com/practice-areas/data-protection-laws-and-regulations/switzerland

Because of its geographic location, most Swiss companies export to the European Union and so even if GDPR is not directly applicable inside Switzerland, these Swiss companies still have to respect the GDPR. This is a good discussion of the issues:

- http://blog.vischer.com/en/the-gdpr-and-switzerland-10-myths-and-misconceptions

What about GDPR and BREXIT?

Honestly? I don't know. And neither does anyone else. It is a mess. As of early April 2019, it is still very unclear what BREXIT will bring in relation to GDPR and data privacy in general. It is very clear that this is one (of the many) topics which has not

been properly managed or planned for, but is very likely to quickly cause serious problems soon after BREXIT happens.

Name other regulations similar to GDPR that exists around the world.

California has created the California Consumer Privacy Act (CCPA), which is substantially similar to the GDPR. CCPA comes into force on 1st January, 2020 – are you ready? Details here:

- https://www.caprivacy.org/

This is a good comparison of CCPA and GDPR:

- https://www.exonar.com/ccpa/#av-layout-grid-6

What do you think of the idea of implementing GDPR worldwide?

That is an excellent idea. Even if countries around the world do not implement GDPR, international companies should. More and more countries outside Europe are adopting GDPR-like regulation, so it is very likely in years to come international companies will have to deal with GDPR-like regulation more often. Hence it make eminent sense now to implement GDPR compliance in all their computing systems and business processes worldwide now.

Also, customers like it – so it will become a business advantage, if marketed correctly.