




25 REAL QUESTIONS & ANSWERS ABOUT GDPR

 Peter Galdies, Development Director, DQM GRC responds to the top 25 questions asked at the webinar hosted by DataIQ during November 2016. Please note that the responses below represent our views only and should not be viewed as legal advice. We hope that you find this document useful.

Will the GDPR apply to all SMEs or only ones over a certain size?

The GDPR applies to any organisation collecting or processing personal information on EU residents regardless of an organisation's size. There are some small exceptions from the requirements (for example, regarding documentation) for organisations of less than 250 employees – but these are also caveated and quite minor in impact. There is an intention to further mitigate impact on smaller organisations – but this should arrive in the form of clarification and advice from the supervisory authorities over time. Our advice right now would be to assume that it applies to any organisation

Will data protection officers (DPOs) not always be required depending on the business type or size?

This is correct – public authorities, anyone carrying out “regular and systematic processing of data subjects on a large scale”, or where core activities rely on large scale processing of special categories or personal information (as in health, racial, ethnic, political, religious, philosophical, trade union, biometric, sex life & orientation) must have a designated data protection officer.

Organisations where this is not the case should consider this carefully. In many cases it may prove useful to organisations to have someone performing similar duties even where not strictly necessary, as implementation of data protection law now requires more detailed knowledge and business process than previously needed.

Could the DPO for a business be a third-party provider? Do companies exist that will provide external DPO support?

Yes – the DPO does not have to be a full time, dedicated employee although consideration should be given to this in organisations where the work is likely to form such a role. The DPO may be a staff member or fulfil their tasks via a service contract and can undertake other duties – but these must not conflict with their DPO responsibilities.

It's also worth considering that DPOs must also be provided with the independence, authority and resources to fulfill their duties – and how might this work as a third party contractor?

DPOs can even be shared across several organisations or undertakings. Many organisations, including our own, will be able to provide such support.

Do you believe that a business will be able to qualify for a certificate or accreditation (like an ISO mark) that shows they are conforming to the GDPR? Do you think this is something that the ICO or trade bodies are considering?

Absolutely. Article 42 spells out that member

states, the European Data Protection Board and the Commission shall all encourage (particularly at union level) the use of certification, seals and marks for demonstrating compliance. This will be a formal system – controlled and authorised ultimately by the EDPB. We expect the ICO and trade bodies (such as the DMA) to setup, approve and accredit suitable schemes.



Does a specific contact in a company in a business-to-business relationship count as personal data or does it only apply to consumers?

Personal data means any information relating to an identifiable, living, individual person. There is no distinction made as to the context or role of the person – so information about individuals in the business or work setting still counts as personal information and is subject to the Regulation in the same way.

Does the GDPR apply to B2B data in the same way as B2C?

Yes. Processing of personally identifiable information relating to living individuals in the business context is included. Even the business information of micro businesses, such as sole traders, can be included where that information can be recognised as relating to an individual.

Does the GDPR require organisations to notify the data subject when they detect a data breach?

Not necessarily. The Regulation requires the data subject to be notified “when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons”. While we do expect some clarification around this from the regulatory bodies at some point we would recommend that all controllers have a plan for managing such contact in place.

Note that this notification is not required if suitable measures were in place to mitigate the risk prior to the breach e.g. if the data were to be made unintelligible through encryption.

Who is responsible for reporting breaches of hosted services like MS Dynamics Online CRM?

As a processor appointed by a controller they are responsible for notifying the controller, without undue delay, in the event of a breach. It is the controller that is responsible for reporting the breach to the supervisory body which in our case is the ICO.

It is important to note that controllers are responsible for assessing their processor’s capabilities to comply with the Regulation. Although we don’t necessarily believe that this means you must have an in-depth understanding of the technicalities of their platforms, but you must seek assurances that

the processor has adequate processes in place to manage personal data properly. A suitable certification scheme will help here in the future (see previous question).

How does the requirement to notify the ICO of a breach interact with the common law right not to self-incriminate?

We are aware of this potential conflict which has also arisen in other areas of law. It’s really one for the lawyers to establish – but it’s worth noting that the notification of a breach is not necessarily the same thing as admitting guilt over that breach. In many instances breaches happen even after suitable and proportional protections are in place.

“Encryption at rest” isn’t mandatory - is that correct?

Essentially this is correct but it’s not quite that straightforward. The Regulation states that “...the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk...” and then goes on to say that this should include, as appropriate, pseudonymisation, encryption, availability, restoration and testing.

In our view, encryption should be used unless other suitable, compensating controls are in place – for example you might have data resting on a database server in a physically secure environment with good access controls in place. In this scenario encryption is probably not required (and may interfere with the performance of the intended system).

However, in the normal course of events, we would normally expect to see portable devices (laptops etc.) which may contain personal data protected by encryption where possible. Note that these decisions need to consider the state-of-the-art, the cost of implementation and the likelihood and risks to the rights of the data subjects as part of a risk assessment.

What approach would you take to comply with Article 32 - Security of processing. Implementing this will be expensive, how does one decide which of the above to implement?

There is no simple answer to this – you must make a risk assessment considering the state-of-the-art, the cost of implementation, the nature, scope, context and purpose of the processing and the likelihood and risks to the rights of the data subject. It’s important that this decision-making process is documented

and the rationale for including or excluding controls is understood.

Ultimately the security you chose to implement must be appropriate to ensure a level of security appropriate to the risk.

Concerning the Right to Erasure, can you please comment on suppression v erasure for marketing purposes?

In an ideal world, should a data subject ask for their personal information to be erased, a controller should only regain the data subject's personal information again through a route where clear permission has been resupplied therefore removing the need for a suppression file.

The wording in the Regulation is reasonably clear; if a person has requested erasure and there are no existing, legal grounds for the processing, and if the data is no longer necessary for the purposes of collection then the data should be erased.

However, in practice we know this is unlikely to reflect reality and problems are likely to arise.

We hope that there will be some clarification here from the supervisory bodies and that this purpose will be noted as legitimate grounds for processing by organisations – but until then we must assume that this will not be the case.

In practice such a request may fall into a "restriction of processing" rather than a request for erasure – leaving a route open for suppression.

The GDPR seems to apply to a company's suppliers, like cloud CRM providers such as Salesforce etc., but what about CRM software providers who are not hosting the information, just providing the software and licences for installation within your IT estate? Will they be affected?

It's the responsibility of controllers to select, manage and control the tools they choose for the processing of personal data. Software providers themselves do not need to warrant their products as being GDPR compliant – but wise ones could consider how they might achieve this to gain competitive advantage.

Certification schemes may help controllers and processors make such choices in future with clear badging to indicate compliance – until then it's down to controllers to make properly considered choices.

I've read reports that double opt-in consent will be required and others where it is single, is there a clear answer? And if not, why?

Consent is a complex issue – for a start it's only one of several legal reasons for processing (necessity, compliance and legitimate interests of the controller being others).

Where required consent must be freely-

given, clear and in plain language suitable for the intended audience. The purposes for which consent is being gained must be open and transparent.

Consent should be given by "a clear affirmative act" – for example this could include ticking a box or choosing settings. Silence, pre-ticked boxes or inactivity should never constitute consent.

Nowhere does the Regulation mandate what precise form consent must take – only that it must satisfy the criteria above.

This is not a very satisfactory situation as clear advice is what we all need – so we expect the supervisory authorities to make this clearer in due course.

It's also important to remember that there are other regulations (such as PECR which is also being reviewed in the light of GDPR) that can also determine the form that consent might have to take and that these should also be considered.

If a person within a company requests opt-out, does it opt-out the whole company or just the single person within?

If an individual should request that they are no longer to be contacted then this should, in the normal course of events, apply to just that identifiable person – however there are a couple of things to consider:

1) If that individual is in fact a micro business such as a sole trader or partner then the request may well apply to the organisation (as that organisation represents the individual)

2) If an individual has requested that an organisation be stopped it might be a sensible business decision to do this – of course this depends on the context and purpose of the processing and might not be valid in all situations.

In the charity sector, like other businesses, we occasionally profile supporters against publicly available sources so that we can tailor communications. Am I right that we will need explicit consent for this? And how far does it go?

You should ensure that any sources you use to enhance your data have been correctly and transparently permissioned for such a use prior to applying the data.

Should the profiling also rely on data you have collected directly from the data subject then you must also ensure that those data items were also gathered with the correct and transparent purpose.

Ultimately you should ensure that all data items used have a demonstrable history allowing consent for the purpose.

How long does a consent last for? Is it 2, 3 or 4 years?

The GDPR does not mandate a specific

period but seeks to ensure that data subjects clearly understand at the point of collection the purpose and duration of the processing that is to be undertaken i.e. you must explain to the data subject how long you will use the data for and how to object if this is no longer wanted.

It's worth noting that we believe that recommended (or even default) periods of time may be introduced by the supervisory bodies – and periods as short as 6 months are under discussion. This is another area where we will wait for further guidance.

To get all the permissions from customers and prospects aligned with the GDPR, what should we do?

Not a quick or easy question! We would investigate thoroughly and build a specific programme for each client – but in brief:

1) Clearly understand the consents you require.

2) Map your existing consents to this framework and check that these were gathered according to the GDPR requirements – transparent and informed with all the information required under the GDPR available.

3) Change your existing systems to enable them to gather consent at the standard required by GDPR.

4) Build a programme of communication specifically designed to gather consents to the standard required – this will vary from organisation to organisation.

5) Prepare to deal with the fact that your addressable audience may decrease.

Will the soft opt-in clause no longer apply then?

There is no specific "soft opt-in" built into the GDPR but "direct marketing" to customers for similar goods or services will be a legitimate purpose for organisations – meaning that consent is not required.

There are some issues to be resolved here:

1) What does "direct marketing" actually mean? There is some discussion to suggest this might mean "post only", no segmentation, unintelligent DM – this is not unlikely but we must wait for clarification.

2) How this legislation and PECR (which is currently where the soft opt-in mechanism resides) interact is yet to be fully understood.

Is Data Portability for all or is it intended more for banks & utilities?

The regulation states: "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine readable format and have the right to transmit those data to another controller without hindrance..." where the processing is carried out by automated means.

The above statement is complex – but in principle it means that right to data portability applies to many organisations – not least of which are the so-called “information society services” such as social media and other internet based services, price comparison sites, credit checking organisations, utilities, banks, charity donation sites and all services effectively providing “hands off processing” for some, or all, of their services.

Do you expect that the Right to Data Portability will work in a similar way to the account switching mechanism in banking?

We believe that this is one of the long term, more visionary, objectives of the GDPR – to enable much better competition and choice for EU resident consumers by giving potential suppliers all the knowledge they need to tailor their service and product for the individual.

It's worth noting that finely grained transactional data may be included within this definition – not just summary data.

The vision of a smart data-driven information based economy is laudable – but as an organisation ourselves we recognise the challenge this represents.

What are the GDPR implications of a multi-national company doing business in the EU or having customers in the EU?

Simple – the GDPR will apply to the processing they undertake of living EU residents regardless of where the organisation is based or where the processing takes place.

What does “right to restrict processing” mean?

The Regulation defines restriction of processing as “the marking of stored personal data with the aim of limiting their processing in future”. Data subjects can request a “restriction of processing” when;

1) they object to processing such as profiling or marketing – the processing shall be restricted pending the verification of the request– i.e. does the controller have legitimate grounds to override the request or not. Once this decision is made the processing shall either cease or continue and the restriction will be limited.

2) they contest the accuracy of data to allow verification by the controller.

3) the processing is unlawful and the data subject requests restriction rather than erasure – note that if explained clearly to the data subject this might be the correct mechanism to use to allow suppression activity instead of data erasure.

4) the controller or processor no longer requires the data for the original purpose but needs to retain it for the establishment, exercise or defence of legal claims.

The key thing here is the temporary nature of the restriction – it's something that's a way of modifying the use of some PII for a limited



amount of time prior to the change in processing or erasure of the data.

In the normal course of events this is not a right we expect to see exercised often.

What will be the Brexit ramifications regarding GDPR?

We believe that GDPR will go ahead either exactly as is or in a very similar, compatible way. Karen Bradley MP, Secretary of State for Culture, Media and Sport (CMS) in a conference with the CMS Select Committee on 24 October commented:

'We went through a number of matters. An example might be the General Data Protection Regulation, which of course comes into effect in the spring of 2018. We will be members of the EU in 2018 and therefore it would be expected and quite normal for us to opt into the GDPR and then look later at how best we might be able to help British business with data protection while maintaining high levels of protection for members of the public.'

The Information Commissioner, Elizabeth Denham, has further stated in her recent blog on 31 October 2016 'The ICO is committed to assisting businesses and public bodies to prepare to meet the requirements of the GDPR ahead of May 2018 and beyond. Within the next month, we'll publish a revised timeline setting out what areas of guidance we'll be prioritising over the next six months.'

Our understanding is that by May 2018 we will still be in the EU. The government has stated that the most likely approach for "converting" EU laws into English law will be to transcribe them en-mass from European to domestic law and then unpick those we don't want. If this is true then it's highly unlikely that the government will pick on data protection law as something "we don't want" and therefore any changes or revisions are set to be some years down the road.

It is clear that the supervisory authority is pressing ahead which makes us believe that organisations must do the same.

One area in which Brexit may have a more direct impact is the role and inter-relationship of our own supervisory body and the European Data Protection Board. Much of the GDPR is concerned with how these bodies interact and this will need agreement and re-drafting for a "go it alone" supervisory body and local law. This is unlikely to make much tangible change to end-user applicability but may allow for a change in the punitive regime. Ultimately we may end up with different punishments or fines, but these would have to broadly align with the European equivalents.

In any case, it's worth remembering that if your organisation processes (or is likely to process) the personal information of EU residents then all this is irrelevant as the law will apply directly to this processing.

Who enforces GDPR? Is it the UK's Information Commissioner, the equivalent authority within the country whose citizen may have been affected, both, neither or someone else?

Normally a breach will be referred to the supervisory authority located in the member state where the processing is occurring (or exceptionally if the majority of data subjects effected reside within that member state).

If the processing is located outside of a member state and the processor has not already nominated a local office with the EU to handle the complaint then there is a process for the lead authorities of each member state to nominate a single authority to undertake the work. Any dispute here will be resolved by the European Data Protection Board but the locale of the majority of data subjects effected is likely to play a part.



About DQM GRC

Formed in 1996 DQM GRC specialises in data governance, risk mitigation, compliance advisory services, research and technologies to de-risk data assets and help clients use their data to drive business performance. It provides consulting, research, and data protection products and a unique, proprietary technology & data governance platform for tracking data flows.

DQM GRC is the market leader for protecting and improving valuable data assets in the important commercial, customer and marketing data sectors. Over 80% of major commercial data owners, including BT, Callcredit, D&B, Equifax, Experian and Royal Mail rely on DQM GRC to protect their data assets. Increasingly, major brands from finance, retail, media, not for profit, and telecoms are now selecting DQM GRC too.

The company has a respected position in the market, winning 9 industry awards, sitting on the data councils of the DMA, IDM and techUK and Boards of the DM Commission and DM Foundation. The introduction of major new EU General Data Protection Regulation (GDPR) in 2016 is driving interest from customers who need help to meet the demands of the new regulation..

DQM GRC with its proprietary solutions and expertise is well placed to strengthen its leadership position. We support FTSE 100, large and mid-market organisations across the UK and internationally.

For more information on how DQM GRC can support your business call Christine Andrews on 01494 442900 or email her at christine.andrews@dqmgrc.com



DQM GRC

DQM House
Baker street
High Wycombe
HP11 2RX

T: 01494 442900

www.dqmgrc.com

DQM GRC is a trading name of Data Quality Management Group Ltd