

## Cobweb's GDPR webinar Thursday 22 June 2017 – Qs&As

Pierre Westphal, independent GDPR Implementation Consultant and webinar host answers your questions.

Please note, many questions were complex, and would be particularly suited to discussion during a [Consultant-led Assessment Workshop](#)\*

### 1. Will Brexit affect the GDPR requirements?

Pierre: The ICO has taken position on the impact of Brexit. The last announcement, confirmed during the Queen's Speech last week, states that Brexit should not impact GDPR requirements for the following reasons:

1. GDPR comes into force 25 May 2018. Brexit won't happen before and until then all EU laws apply.
2. GDPR applies to EU citizens' data regardless of where the controlling or processing of that data takes place, which means that countries outside the EU (including the US and an independent UK) would have to apply GDPR for client data where the client is in the EU.
3. The UK would have to introduce an equal replacement if it decided to revert to existing DP regulations, which would simply be GDPR under a different name.
4. The UK is aiming to match the GDPR standard to attract global data centric business.

### 2. What is the definition of 'Client Data? For example, an Outlook business card?

Pierre: In the GDPR we talk about Personal Data, not Client Data. As per article 4 of the GDPR, **Personal Data means any information relating to an identified or identifiable natural person (individual).**

An identifiable **natural person** is one **who can be identified, directly or indirectly**, in particular by reference to an identifier such as a name, an identification number, location data, **an online identifier (IP)** or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. If the Client Data is a natural person who can be identified by reference to its name, then this would fall under the GDPR. If the Client data is a Company, then it would not fall under the GDPR.

### 3. What is the impact of the right to withdraw consent or restrict processing for a patient participating in a medical study?

Under GDPR article 9 (2.h), the processing of personal data that reveals information about health is not processing sensitive data if the processing is necessary for the purposes of preventive or occupational medicine, medical diagnosis, the provision of

health or social care or treatment, or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional.

Which means that consent would not be required. However, Member States are entitled, under Article 9(4) GDPR, to maintain or impose further conditions (including limitations) in respect of genetic, biometric or health data. Entities that process these categories of data should continue to keep the development of relevant national law under review and consider the need for further lobbying work in this area. Should continue to keep the development of relevant national law under review and consider the need for further lobbying work in this area.

**4. I'm assuming that GDPR applies to any size business as long as they have client personal data - correct?**

Pierre: Correct, but not only client personal data. It also includes employees' personal data.

**5. Can you advise if this purely relates to website interaction rather than paper-based documents and/or emails?**

Pierre: Personal Data 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 the 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; on a computer or not.

So, paper-based documents and emails fall under the Personal Data processing.

**6. I didn't understand the 'cloud' comment, as that's where data is stored, not processed.**

Pierre: I'm afraid I'm not sure I understand the comment, but I assume it refers to where the data is processed.

Data 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; on a computer or not.

**7. Re B2B database contacts: Our company requires consent from the other company to continue connecting with them. How do we do that? Email? We find we can get a low percentage of replies via this way and are afraid that we might lose a lot of contacts.**

Pierre: GDPR doesn't apply to companies, but to individuals. If your customer contacts are companies, it won't fall under the GDPR definition.

**8. In general, we don't deal with private customers – it is mostly B2B. However, we do employ full ID pass holders and are instrumental in getting their security passes for airports. The fact that we then retain all the information they have given us – would we be liable to comply with GDPR?**

Pierre: Yes, the list of full ID pass holders should be considered as a personal data and as such would be liable to comply with GDPR. As a controller, you should make sure the controller principles are met.

**9. I have many contacts in my system already – how do I maintain compliance? Do I need to obtain consent from all 'legacy' contacts?**

Pierre: Not necessarily, it would depend on the personal data you hold and the purpose of your processing.

This should definitively be addressed as a second step during an Assessment Workshop with the following actions:

- Data assessment
- Application of the principles to any processing of Personal Data as a controller
- Investigation as to whether sensitive data is being processed?
- Is there a consent requirement?

**10. Many customers call into my technical support desk. Do I need to gain explicit consent from each individual who calls in, or just the business (my customer) they work for?**

Pierre: Explicit consent is only required for sensitive data processing, data transfer to the US and for children under 16. But, before engaging with the individual, your

company must inform in a transparent way the individual of the purpose of the information processed. But again, depending on the type of data your company is processing, a Data Assessment would be required to better understand how your technical support calling process is liable to the GDPR.

### **\*Consultant-led GDPR workshops, assessments, clinics and bespoke days**

At Cobweb, we're doing all we can to help customers understand GDPR requirements and ensure compliance, and are offering the following consultant-led sessions (full details can be seen [on our website](#)):

- GDPR Workshops
  - (Open: £150 pp/ Corporate £1,400 per day)
- GDPR Assessment Workshops
  - (Corporate £1,500 per day)
- GDPR Clinics
  - (Corporate £1,500 per day)
- (+ GDPR Additional Consulting Day (£1,100 per day))

cobweb

LIBERATING TECHNOLOGY

As a first step – if you haven't already, take Cobweb's [GDPR readiness survey](#) to see how ready you are for GDPR. Our sales team will take you through the 15 key-point survey, created by Pierre Westphal.

We've also created a GDPR hub where we are collating useful pieces of information generally available, as well posting items we have created, such as ebooks and blogs.

Copyright © Cobweb Solutions Limited. All Rights Reserved.

Registered address: Cobweb Solutions Ltd, Delme 3, Delme Place, Cams Hill Estate, Fareham, Hampshire, PO16 8UX, United Kingdom.

Company Registration no: 3283443; VAT no: 682251241

T: 0330 057 2287

[www.cobweb.com](http://www.cobweb.com)

[hello@cobweb.com](mailto:hello@cobweb.com)