Data Retention Webinar: Q&A

Is data retention schedule a document that's required by GDPR, and what information should be included in it?

Data retention schedules are not explicitly required by the GDPR. What GDPR requires, is to establish data retention periods which you can document either in your records of processing activities, data retention policy, data retention schedules, data handling policy or any other document.

Have you got any examples of instances when "Legitimate Interest" has been used as a basis for processing? And have you got examples where this has been challenged?

In fact, we have been discussing legitimate interest as a legal basis in our previous webinar. If you would like to know more on this, please check it out.

In a nutshell, we often see legitimate interest used for the processing of B2B data, e.g. whilst you are carrying out business development activities. Another example is marketing to existing customers. The latter is often (wrongly) thought to require consent rather than a legitimate interest.

If for example a customer makes a complaint and we record it, and we have to keep the employee data for 6 years and the customers data related to that complaint needs to be kept for 21 years, do we need to separate that data, in order to destroy the employee data after 6 years?

Generally, information that needs to be kept for different purposes and different time periods should be stored separately.

However, it seems you are talking about where a customers' complaint relates to a particular employee, and a record of that complaint needs to be kept annexed to the employee's file for disciplinary processes. In such a situation, you would keep the record that a complaint was made about the employee but would not need to identify the name of the customer that made the complaint.

If you have, over the years, captured large quantities of photographs of people, both staff and the public, a large percentage of which are not necessarily accompanied by consent forms - are you required to delete them all immediately?

We always recommend carrying out a regular review of personal data that is being processed in order to ensure that there is no legacy data left. It is good practice to carry out this exercise at least once a year. In case of photos collected without consent, if you are not able to rely on a legitimate interest for them, you would definitely need to dispose of such data.

I've a Sunday school as a client. They process child data to provide their services - name, ICE etc. They retain SOME of the data after the child leaves - name, year of birth and attendance record - in case of an abuse claim - i.e. Legitimate interest. Does this mean 2 lines on the Data inventory / RoPA for each data element: one for initial purpose, and one for the retention purpose?

Indeed, that's correct – one line on ROPA would define your initial processing purpose and the second line will describe the details on continuous retention. Most likely here you would have two differing legal bases.

Has it been considered that data-mapping could itself form a risk? E.g. if a doc is created which details the locations of all the sensitive info a company holds - if that gets in the wrong hands it would make it very easy to find the sensitive info...

In a data mapping exercise, which feeds into a Record of Processing Activities, the information on 1) types of data processed and 2) the location of the data and 3) access controls would only be mentioned generally. ***Only information required to be recorded in the ROPA should be recorded*** – such as the types of personal data (e.g. list 'Name' or 'contact details', 2) the location - (e.g. 'Salesforce' or 'company file server') and 3) access controls (e.g. 'limited to HR team')

Will a legal retention period always override any other GDPR related retention periods?

Unfortunately, GDPR does not establish specific data retention periods, we only have a couple of generic examples in the recitals of the GDPR. However, the recitals can only be treated as recommendations rather than requirements for compliance. Thus, you would always have to refer to specific laws for retention periods.

We have a data warehouse running in a private data centre. We want to move it to the cloud. Do we need to inform our customers of the change of processing? Data retention will not change.

Not likely. You may only have to notify them of the migration if it involves processing data outside of the EEA, for example.

Why do cookies relate to Accident records? (slide 21)

Apologies, this was a spelling mistake. Cookies do not relate to accident records by any means. Slide now amended.

Which guidance do the marketing retention periods in your slide come from?

These come specifically from the ICO and French data protection authority (CNIL).

Is there a good source for typical retention periods for guidance - I used to use the National Archives, but this is no longer updated?

Retention requirements will vary between the country in which you operate and the sector/specific legislation that you are subject to. Essentially, the best way to achieve this would be to locate the specific legislation (although this is very time consuming). In addition, there are research tools than you can use to locate this information. You can also contact us for more information on specific retention requirements and drafting retention policies.

How do data retention periods affect customer's right to erasure? Additionally, would be interested to understand when a DPIA would be required. For example, when changing systems that handle customer data or when there are projects taking place.

The right to erasure is limited during the data retention period. The data subject can challenge the retention if you are relying on legitimate interest to process the data, in which case you will have to evaluate and justified the continued retention.

A DPIA is required where the data processing is likely to result in a high risk to the rights and freedoms of individuals, as established by Article 35 of the GDPR. Supervisory authorities have provided guidance on the

situations where DPIAs are to be conducted, which generally includes situations such as CCTV monitoring, employee monitoring, processing biometric data, making automated decisions with respect to data subjects, etc. We have covered this topic in our GemTalk #2 Webinar on Privacy by Design.

If a company keep employee's data in the cloud or in HQ EU country server, in other countries subsidiaries will need employees' consent for this?

Generally any transfer of personal data outside of the EU will need to comply with specific safeguards, including to check that the transfer is to a country that the European Commission has declared 'adequate', that the data is transferred pursuant to Standard Contractual Clauses, or in exceptional circumstances, consent. Consent should generally not be used to allow subsidiaries to access employees' personal data.

CONTACT US

If you would like to speak to our consultants to discuss how we can help you with data retention questions, then please email the data protection team (dataprotection@gemserv.com) or speak to a member of the team on +44(0) 207 090 1091.