The General Data Protection Regulation ("GDPR"): What does it mean for Confirmit’s clients?

About this document

This document is intended to share Confirmit’s understanding of this subject matter. This document must not be interpreted as legal guidance. We recommend that you seek your own legal advice on this matter and monitor this space closely.

What is the issue?

Data protection laws in the European Union (the "EU") are currently governed by EU Directive 95/46/EC (the "Data Protection Directive"). This Directive also applies to the broader group of countries referred to as the European Economic Area, the "EEA", which includes EU countries as well as Iceland, Liechtenstein, and Norway. Confirmit’s headquarters are in Oslo, Norway.


Whereas a Directive needs to be implemented into state law in each EEA country and may therefore be subject to country-specific amendments, a Regulation is intended to be used “as is” across EEA countries. Although the reality is that state-by-state adaptations will still take place to a certain extent, the key purpose of having this as a Regulation rather than a Directive, is to achieve increased harmonization of data protection practices throughout the EEA zone.

What is the overall purpose of the GDPR?

The overall purpose of the GDPR is to protect the personal data of EEA citizens. The GDPR provides data subjects with rights in relation to personal data they have shared with businesses that collect, store, and process such personal data.

Who does the GDPR apply to?

Every company collecting personal data from EEA citizens is subject to the GDPR. A company does not need to be established in the EEA to be subject to the GDPR terms. If you are located outside of the EEA and collect personal data from the EEA, the GDPR applies to you.
Controllers & processors

The GDPR discerns between two key roles companies may have. A company may act as a data controller or it may act as a data processor (or both). The data controller is the party determining what data is to be collected, from whom, how it is to be collected, and how it is to be used. The data processor executes the instructions of the data controller either manually or programmatically, for example via a software-as-a-service offering such as the Horizons SaaS.

In respect to our clients Confirmit acts as the data processor, whereas our clients have the role of data controllers.

The seven GDRP principles

Under the GDPR, data processing must involve:

1. **Lawful, fair, and transparent processing** – emphasizing transparency for data subjects
2. **Purpose limitation** – having a lawful and legitimate purpose for processing the information in the first place
3. **Data minimization** – ensuring data is adequate, relevant and limited, and organizations are capturing the minimum amount of data needed to fulfill the specified purpose
4. **Accurate and up-to-date processing** – requiring data controllers to make sure information remains accurate, valid, and fit for purpose
5. **Limitation of storage in a form that permits identification** – discouraging unnecessary data redundancy and replication
6. **Confidential and secure** – protecting the integrity and privacy of data by making sure it is secure, which extends to IT systems, paper records, and physical security
7. **Accountability and liability** – demonstrating compliance

Confirmit will be GDPR-Ready well ahead of May 2018

Confirmit has been conducting GDPR-Ready initiatives since the fall of 2016. In most areas, Confirmit is now GDPR-compliant. We are further ensuring that by the time the GDPR comes into effect, the responsibilities of Confirmit in its roles as the data processor (in relation to personal data we process under instruction of our clients) and as a data controller (when collecting data on our own initiative) are fully met. We are following developments closely as more guidance is being published by the European Data Protection Supervisor (formerly Article 29 Working Party) in relation to the GDPR.

We have been mapping the GDPR clauses towards our operations thoroughly, both in relation to our role as data processor, and that as a data controller. Further, we are focusing on further improving the Horizons Software in order to better facilitate the tasks the GDPR requires you as a data controller to be responsible for. See Appendix 2 for the full listing.
Confirmit has already in place a Privacy Shield certification via the US Department Of Commerce, and TRUSTé Enterprise Privacy Certification in accordance with EU laws. As a client of TRUSTé (now TrustArc) we obtain ongoing guidance in relation to compliance. Further, via our long-time legal partners at Taylor Wessing in the UK, we receive frequent newsletters providing the latest updates on regulatory matters related to data privacy and compliance. We also work with Lawyer firm Føyen Torkildsen in Oslo.

Click here for a 30-minutes WebCast offered by Confirmit together with Føyen on August 29th 2017. Confirmit’s COO offers a short update of our company’s efforts from minute 24.

Some useful sites addressing data protection and privacy laws

Our UL lawyers at Taylor Wessing offer public access to a wealth of useful data protection information, at their Global Data Hub: https://www.taylorwessing.com/globaldatahub/. Thorough GDPR checklists are available there. Particularly recommended overall outlines:

- Checklist of Processor vs Controller
- Obligations of Data Processor:
- Obligations of Data Controller:

You may also wish to subscribe to their free-of-charge newsletters, https://united- kingdom.taylorwessing.com/en/myhome/signup

In the UK, the Information Commissioner’s Officer (ICO) provides ongoing guidance in this area. Although the ICO does not represent other EEA countries, they do offer interesting guidance. Here are a few pieces we recommend:


White & Case (http://www.whitecase.com/) have published a very thorough and detailed mapping of GDPR impact on companies. We recommend looking into the following in particular:


Hunton & Williams published a good 30-minutes summary of GDPR on June 19th here: https://www.youtube.com/watch?v=EDljMF_aHmg
APPENDIX 1
Questions & Answers

Note: Data controller: you. Data processor: Confirmit.

Q: When does the GDPR come into effect?

Q: Should my company take any actions before the GDPR comes into effect?
A: Yes. All companies handling personal data originating from the EEA will need to take required actions. The first step is to perform a thorough analysis of how the GDPR may impact your operations. Since the GDPR does not entail transitional arrangements, it will have effect from day one, so companies will need to be ready by May 25th 2018.

Q: Can Confirmit help me with my GDPR readiness program?
A: No, this is unfortunately not a service we are able to provide. However, there is a whole ecosystem of companies specialized in assisting firms in their efforts to become compliant. They include lawyer firms such as the ones mentioned above, data security and compliance companies, and industry organizations. One example is the cooperation between IAPP and TrusArc, https://www.trustarc.com/products/iapp-gdpr-readiness-assessment/. A quick search on the web will help you find many more.

Q: Obtaining consent from data subjects is key under the GDPR. Who is responsible for that?
A: The data controller is fully responsible for obtaining consent, and Article 13 of the GDPR is core to this. The Horizons Software enables you to create a consent page and obtain the approval via a question. For the UK, guidance in relation to consent is provided by the UK ICO here, and a new an updated version is announced for December 2017. It is also expected that the EU will issue more guidance.

Q: Does the GDPR also apply to anonymous data collection?
A: No. However, the GDPR has extended the definition of what is defined as personal data and includes for example data that together with other data can enable identification of data subjects.

Q: Our company is not collecting any personal data originating from the EEA. Does the GDPR apply to us?
A: No. It is however being debated whether the GDPR requirements apply also to data collected from EEA citizens located outside of the EEA. From a practical point of view, we believe it would be difficult for the EEA to enforce this towards companies outside the EEA.
Q: Does data collected from data subjects based in the EU or EEA have to be stored on servers in the EU or EEA?

A: No. There is no localization requirement under the GDPR. The GDPR requirements relate to the adequacy of the operational, technical and security measures in place with the parties processing the personal data outside of the EEA.

Q: Are any countries outside of the EEA already approved by the EU as “safe countries” for the processing of personal data originating from the EEA?


Q: Our business is US based, but it is not Privacy Shield certified. Does that prevent us from processing data from the EEA?

A: Currently no, and we are not aware of plans for requirements of Privacy Shield registration under the GDPR. Companies in the US can process EEA personal data provided that they comply with the requirements of the GDPR. That said, you may experience increasing demand for more thorough data processing agreements between you and your end clients.

Q: Our business is based outside of the US and EEA and in a country not included in the EU list of approved third countries (see URL above). Does that prevent us from processing data from the EEA?

A: No. Companies anywhere in the world can process EEA personal data provided they comply with the requirements of the GDPR.

Q: Where is Horizons data stored?

A: Confirmit offers three different Horizons SaaS hosting environments, one in the EEA in London, England, one in Sydney, Australia, and one in Dallas, Texas in the US. The data is isolated on each site, there is no automatic transfer between them. Some of our clients use more than one hosting environment, either to improve performance by increasing proximity to the users to reduce internet latency or because of compliance considerations.

The Horizons SaaS hosting environments are not “cloud” as is the case for many other vendors. Our Horizons SaaS hosting environments store the data physically in a specific datacenter, and the management of the datacenter draws on the vast resources of the industry-leading hosting provider, Rackspace. Rackspace is recognized as world-leading in managed hosting; it holds a number of security certifications, including ISO27001, Payment Card Industry, and ISO 9001 and is SOC II audited in accordance with SSAE16 / ISAE3402. See http://www.rackspace.co.uk/certifications for the UK, and the Compliance and Validation section of http://www.rackspace.com/security/management for the US.

Q: Is Confirmit’s back-up model for the SaaS Service aligned with the requirements of the GDPR?

A. The GDPR does not go into detail about how back-ups are to be performed. Confirmit follows models consistent with industry standards. The back-up model we offer for each of the SaaS sites is set forth in the agreement we have entered into with you as a client. It normally entails daily incremental back-ups, and weekly
full backups encrypted AES-256 and stored offsite with a specialized third party (for our UK and the US sites, Iron Mountain). Iron Mountain does not have access to the encryption key, so the data is irretrievable and without value as long as it remains stored there or elsewhere. After 52 weeks offsite, the back-up media is repurposed for back-ups of the latest data (52-weeks rotation) and the old data is overwritten. Only when the back-up tapes are sent back to the data center, would Rackspace, the party holding the encryption key, be able to retrieve data.

As it pertains to the GDPR and concepts such as those in articles 16 (rectification), 17 (right to be forgotten) and 18 (restriction of processing), there is no guidance from the European Data Protection Supervisor / Article 29 Working Party in relation to whether those rights also apply to encrypted backups. Accordingly, the consensus so far is that as long as the back-ups are encrypted and the holder of the back-ups does not possess the key, the purposes of the GDPR in relation to data protection are met (encrypted offsite back-ups are “blocked from further processing” by default). In the event you as our client were to invoke the retrieval of datasets from back-ups, and to the extent you have applied edits to data records on the equivalent datasets stored on the production environment on the basis of data subject requests under the GDPR, you must make sure to apply the same changes also to the data retrieved from back-up.

**Q: Does the GDPR introduce a requirement for all data to be encrypted at rest?**

A. No. Encryption is one option listed in the GDPR, but it is not a requirement. See #32 of Appendix 2 for details. That said, Confirmit offers the ability to encrypt data, see this page.

**Q: Does Confirmit meet its current obligations in relation to data protection? Can I see documentation of that?**

A: Yes. Article 32 of the GDPR puts an obligation on both controller and processor to have “appropriate technical and organizational measures to ensure a level of security appropriate to the risk”. Confirmit fully meets this requirement. For an overview of the organizational and technical measures we have in place to protect personal data stored on the Horizons SaaS, please download the PPT from here (Horizons Security PowerPoint). Further detailed documentation, including reports from third party security reviews of the SaaS Service and of the Horizons Software, will be provided on request.

Confirmit will to the extent necessary update its measures to meet new requirements under the GDPR and other laws applicable to our role as data processor.

**Q: Is Confirmit audited in accordance with ISAE3402 / SSAE 18 (formerly SSAE16), SOC2 Type 1 and Type 2?**

A: As of the fall of 2017 Confirmit is undergoing such auditing. We plan to have completed Type 1 by Q4 2017, and Type 2 by Q1 2018. The auditing is performed by Armanino in the US. We will share the reports with our clients on request.

**Q: Does the GDPR require us to sign a new agreement with Confirmit, or to enter into separate data processing agreements?**

A: No. The GDPR does not set forth the need for signing a new agreement; the requirement is that there needs to be a written agreement in place aligned with the requirements of the GDPR. The current agreement already in place between Confirmit and its clients already addresses the majority of the GDPR requirements. Confirmit is currently preparing a GDPR addendum which we will offer for signature to our existing clients in order to fully meet the new GDPR requirements.
**Q: Does the GDPR require us to sign any agreements directly with Confirmit’s subcontractors?**

A: No. The GDPR does not introduce a requirement for Confirmit’s subcontractors to sign up directly with each of our clients individually. Quite the opposite; the GDPR provides clear guidance in relation to the responsibility we, as the data processor, have in relation to this. For example, article 28.2 states that we cannot use a sub-processor unless you authorize it. Our use of our data center provider Rackspace has already been authorized by you under the existing SaaS Agreement.

As per article 28.4 of the GDPR, Confirmit must include GDPR related responsibilities into its agreement with its subcontractors, and this is already in place. Confirmit will remain responsible for the acts and omissions of the sub-processors.

**Q: Who is responsible for the deletion of personal data?**

A: The data controller is. GDPR states that personal data should not be kept for longer than is necessary. As a data processor we are in no position to assess how long “necessary” is; that is the responsibility of you as the data controller. You can at all times delete data on the SaaS site, and we will delete data upon expiration of the Agreement we have in place with your company in accordance with the terms set forth therein.

**Q: Will Confirmit respond directly to data subjects in the event they contact Confirmit to assert any of their rights (access, rectification, erasure / forgotten, etc) under the GDPR?**

A: No. Articles 15 to 20 are all referring to the data subjects’ “right to obtain from the controller”. Confirmit is not the controller, and is therefore not authorized to act on such requests. Confirmit is the data processor and must therefore only act on the instructions of the data controller (you – our client) in relation to the personal data Confirmit processes for you. Should Confirmit receive requests from data subjects under the GDPR, or under any other laws applicable to personal data, we will always refer the request back to the data controller (you - our client) unless applicable laws prevent us to do so. You will be able to handle the requests yourself via the self-service SaaS service (see details in Appendix 2, especially 15.1, 16 and 17), or you may reach out to us for assistance.

**Q: Does Confirmit have a procedure for handling complaints raised by data subjects in relation to personal data it processes?**

A: Yes. Complaints would normally be processed via the TrustARC’s Privacy Dispute Resolution portal, which is referred to amongst others from Confirmit’s Privacy Policy, alternatively by e-mail to a number of addresses we maintain. Should the complaint relate to a data subject for which a client of ours is the data controller, we will hand over the case to such data controller as required by applicable law.

**Q: How is Brexit impacting Confirmit’s UK based SaaS? Will Confirmit set up a new SaaS server within the EU but outside of the UK (for example in Germany)?**

A. We are keeping a very close eye on developments in this area, supported by guidance from our lawyers. The situation is currently that the UK has invoked Article 50 (March 2017) and now has two years to negotiate the terms of separation from the EU. It is therefore expected that the UK will leave the EU at the earliest in March 2019. The actual timeline will depend on the progress of what is expected to be lengthy and complex negotiations on the UK’s relationship with Europe and its trade agreements.

As long as the UK remains a member of the EU, personal data is protected in the same way in the UK as in all other EU countries, currently in accordance with the Data Protection Directive, and from May 2018 in
accordance with the GDPR. There is no legal argument not to continue using SaaS environments in the UK at present.

Here are the three most likely scenarios of the Brexit, in order of priority, as they pertain to the processing of personal data:

1. By the time the UK exits the EU, the EU agrees that the UK meets the adequacy requirements in relation to the data protection of personal data. Accordingly, the UK would appear on the list of approved jurisdictions together with countries that are already approved.
   - This would mean that nothing changes compared to today; data can be stored / processed in the UK and on the Horizons SaaS located there exactly as is the case today.

2. If the UK fails to achieve #1, the UK may take the approach that the US has taken and negotiate a side agreement along the lines of the Privacy Shield. Confirmit would subscribe to this regime, exactly as we have done already in the US.
   - This would mean that nothing changes compared to today; data can be stored / processed in the UK and on the Horizons SaaS located there exactly as is the case today.

3. In the unlikely event the UK fails to achieve #1 and #2, and no other avenue is found by the UK to convince the EU that it provides adequate measures for the processing of personal data in the UK, Confirmit would set up a SaaS site in a country within the EU when the UK leaves.

Our view is that it is highly unlikely that the UK will fail to find a solution to this, exactly as the US worked very hard to find a solution. The reason being that the UK has significant commercial interest in making sure that personal data can continue to be stored and processed in the UK even after Brexit. The negative economic consequences of a failure to find a solution would be major to the UK. This view is supported by the Queen’s Speech to Parliament on June 21st 2017 where on behalf of the UK Government it is confirmed that the UK will implement the GDPR.
## APPENDIX 2

### How Confirmit, and the Horizons software, meet / will meet the GDPR requirements

<table>
<thead>
<tr>
<th>Topic</th>
<th>GDPR refer.</th>
<th>GDPR wording</th>
<th>Confirmit’s position for the Horizons software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall purpose of GDPR</td>
<td>1</td>
<td>The GDPR lays down rules relating to the protection of natural persons with regard to the processing of personal data</td>
<td>The Confirmit platform handles different types of data; from customers, employees, and from general market or social research through surveys, web scraping or importing data from other systems. The type of data collected depends on the data collection method and analysis needs, and is fully controlled by the data controller (you). The system provides options for totally anonymized data collection (for example open surveys or surveys with external respondent generation), but for certain types of data collection, personal data is required, for example to send survey invitations via email or to call a respondent for a phone interview (CATI). The SaaS software is unable to assess whether or not data fields contain personal data, so it is up to the users to decide whether to include personal data, depending on research needs.</td>
</tr>
<tr>
<td>Accountability</td>
<td>5</td>
<td>...collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes... limited to what is necessary in relation to the purposes ... kept up to date ...kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').</td>
<td>As it relates to the requirement of keeping data “no longer than necessary”, this is the responsibility of the data controller. As the data processor, Confirmit will process data solely in accordance with the data controller’s instructions. Data controllers can at all times delete records, partial or full datasets from the Horizons SaaS at their own initiative. Further, Confirmit will soon offer the ability to transform the data records such that they will be anonymous, so that they no longer fall under the GDPR requirements, see comment to Article 11 below.</td>
</tr>
</tbody>
</table>
| Consent | 6, 7, etc. | Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her... | Out of all requirements under the GDPR, this is, in our view, the key one for data controllers to be on top of from day 1. Consent is the sole responsibility of the data controller. Specific requirements are set forth in the GDPR in relation to the modalities for obtaining a valid consent, and enabling updates thereof.  
- Consent question can simply be built in the start of the survey.  
- Horizons also offers the ability to set a flag at respondent level to e.g. exclude the respondent record from processing.  
  - See explanation for #18 below  
- Horizons offers an Opt-Out feature. |
<p>| Processing which does not require identification | 11 | A majority of the data analysis and reporting that data controllers carry out in Horizons, does not require personal data (for example aggregated reporting). Where personal data is needed for performing data collection (for example for sending email invites and reminders), there are data editing capabilities provided in the tool (respondent data editor and data processing rules) that allow the removal of personal data |</p>
<table>
<thead>
<tr>
<th>GDPR Right</th>
<th>Paragraph</th>
<th>Confirmit Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right of access by the data subject</td>
<td>15.1 The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information</td>
<td>As a data controller using the Horizons platform you are already today able to export, at your self-service initiative, data-files from the system using standard data export functionality, which can be filtered so that it only provides responses from specific individuals. This can be done for surveys in production as well as archived surveys. If in the future you use the personal data removal features we will be offering (ref 11 above), this whole requirement falls away.</td>
</tr>
<tr>
<td>Right to rectification</td>
<td>16 ...data subject shall have the right to obtain ... the rectification of inaccurate personal data concerning him or her.</td>
<td>Already today you are able to edit data in Horizons, on a self-service basis, via existing functionality: Data editing capabilities are provided in the tool, such as respondent data editor, survey data editor, and the capability to import updated data from file to correct inaccurate personal data. If in the future you use the personal data removal features we will be offering (ref 11 above), this whole requirement falls away.</td>
</tr>
<tr>
<td>Right to erasure (Right to be forgotten)</td>
<td>17 ...right to obtain ... the erasure of personal data ... without undue delay ... where one of the following grounds applies (several grounds)</td>
<td>Already today you are able, self-service on the SaaS, to delete either full data sets, individual data-records, whole questions / variables, or cells in data-records, using existing functionality. This can be done through the data editing capabilities provided in the tool, such as respondent data editor, survey data editor, and via data processing rules. If in the future you use the personal data removal features we will be offering (ref 11 above), this whole requirement falls away.</td>
</tr>
<tr>
<td>Restriction of processing</td>
<td>18 ...right to obtain ... restriction of processing where one of the following applies (several grounds). Where processing has been restricted (as above), such personal data shall, with the exception of storage, only be processed with the data subject’s consent</td>
<td>Horizons already supports the ability to add a custom variable to survey data so that a record can be excluded when data is loaded to reporting databases in SmartHub/Reporting data (InvalidResp).</td>
</tr>
<tr>
<td>Right to data portability</td>
<td>20 ...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</td>
<td>You are already today able to export data-files from Confirmit in a range of different formats using standard data export functionality, which can be filtered to provide only responses from specific individuals. This right can be invoked in addition</td>
</tr>
</tbody>
</table>

Once data collection is completed and the personal data is no longer needed.

Further development underway:
- For ad-hoc surveys, we will be developing capabilities for anonymizing survey responses (at record level) while retaining the non-personal data for purposes of e.g. benchmarks.
- For panel surveys, we will be developing capabilities to “break the link” between panelists and their survey responses.

Once data records / survey responses no longer contain personal data, they no longer fall under the requirements of the GDPR.
<table>
<thead>
<tr>
<th><strong>Automated individual decision-making, including profiling</strong></th>
<th>21+22</th>
<th>Not applicable. Article 71 of the preambles of the GDPR makes it clear that this clause falls outside of the scope of the software and services solutions Confirmit offers.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Protection by design and by default / Data minimization</strong></td>
<td>25</td>
<td>Privacy by design, and data minimization, are the responsibility of the data controller. It is the controller who defines the processes of data collection, and the amount of data to be collected. Confirmit will contribute with information about the technical and organizational measures we have in place to protect the personal data. We have thorough security documentation available, as well as the results of third party security tests of the SaaS service and of the Horizons software. Confirmit will support client audits mandated under the GDPR, see 28 (h) below.</td>
</tr>
<tr>
<td><strong>Use by Confirmit of other processors / subprocessors on behalf of data controller</strong></td>
<td>28.2</td>
<td>Under the scope of the GDPR, Confirmit will inform its clients about the use of sub-processors in relation to personal data. Further, we will ensure subprocessors meet the applicable requirement of the GDPR and in particular paragraphs 2 and 4 of Article 28. Our clients cannot reject the use of the data center provider (currently Rackspace), as it is an integral part of our offering and we cannot provide the SaaS Service without Rackspace. But we accept responsibility for Rackspace’s acts and omissions, and we warrant compliance to applicable data protection laws on their behalf.</td>
</tr>
</tbody>
</table>
| **Deletion and Return of personal data** | 28 (g) | **1. Return.** As this is a self-service SaaS, data controllers can export the data themselves. It is possible to export data from multiple projects (limited to a given number for each export task) through data processing rules by either selecting “all” projects, or assigning a keyword to all projects and using a keyword filter in the data processing rule. Confirmit will upon request assist in exporting data on Client’s behalf as a consulting service.  
**2. Deletion.** Client can delete data on its own initiative at any time during the term. Client is also welcome to provide us with lists of projects that we will delete at no cost. Confirmit will in any event delete data on the SaaS within 60 business days of expiration of the Agreement. SaaS data will remain on back-ups offsite (securely encrypted AES-256, offsite provider does not hold the encryption key) for the duration of the contracted retention period of up to 52 weeks. Such data is deemed as “blocked from further processing” and is therefore not subject to several of the rights of data subject, such as invoking deletion or correction. More details after the table (*). |
| **Appropriate technical measures to protect** | 28 (f), 32 and 36 | Article 32 relates to “security of processing” and article 36 relates to “prior consultation”. We will assist clients to the extent required under the GDPR. Be aware however that “prior consultation” is not necessary unless “the processing results in a risk for the data subject’s rights and freedoms or in the fulfillment of a legal obligation”. |

---

1. Return. As this is a self-service SaaS, data controllers can export the data themselves. It is possible to export data from multiple projects (limited to a given number for each export task) through data processing rules by either selecting “all” projects, or assigning a keyword to all projects and using a keyword filter in the data processing rule. Confirmit will upon request assist in exporting data on Client’s behalf as a consulting service.

2. Deletion. Client can delete data on its own initiative at any time during the term. Client is also welcome to provide us with lists of projects that we will delete at no cost. Confirmit will in any event delete data on the SaaS within 60 business days of expiration of the Agreement. SaaS data will remain on back-ups offsite (securely encrypted AES-256, offsite provider does not hold the encryption key) for the duration of the contracted retention period of up to 52 weeks. Such data is deemed as “blocked from further processing” and is therefore not subject to several of the rights of data subject, such as invoking deletion or correction. More details after the table (*).
<table>
<thead>
<tr>
<th>Section</th>
<th>Duration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>personal data / Prior consultation</td>
<td></td>
<td>information available to the processor would result in high risk in absence of measures taken by controller to mitigate the risk”. Our view is that this is not the case.</td>
</tr>
<tr>
<td>Availability of security information, participation to audits and inspections</td>
<td>28 (h)</td>
<td>... (processor to) make available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.</td>
</tr>
<tr>
<td>Instructions from controller that infringe the GDPR or Member State data protection provisions</td>
<td>28 (h)</td>
<td>At no charge to our clients, we provide a variety of security-related documents, which we update regularly. We also provide access to third party security assessments for the SaaS Service and for the Horizons Software (McAfee / Intel Security, and Veracode). Given the SaaS Service is offered “as is” in accordance with our documentation, and security is thoroughly documented, it is our view that the GDPR does not require individual audits by hundreds of clients. If clients nonetheless request us (and if required, our subcontractors) to undergo audits, we will assist subject to agreement to the conditions of such assistance in advance. The GDPR does not state that such auditing assistance is to be provided by data processor at no cost.</td>
</tr>
<tr>
<td>Record of processing activities</td>
<td>30</td>
<td>... shall maintain a record of processing activities under its responsibility. Requirement both to the controller and to the processor. Easily achieved via a written document.</td>
</tr>
</tbody>
</table>
| Pseudonymisation and encryption                                         | 32       | ...controller and processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate the pseudonymisation and encryption of personal data.  
  - Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;  
  1. Pseudonymisation. We have clients doing this already. In Horizons, they replace personal data in a record set with codes. Then, outside of the SaaS, the list of codes is kept in a format enabling the matching of the codes to individual identifiers. This then permits re-identification of records at a later stage if necessary.  
  Be aware that with pseudonymisation, data can be linked back to the data subject. According to GDPR, pseudonymized data must therefore still be treated as personal data. |
| Personal Data Breach                                                    | 33       | ...means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Note that as the SaaS Service is self-service, it may well be your users (data controllers) who cause the data breach (e.g. by not sufficiently protecting their user credentials). In such cases, Confirmit will cooperate in limiting the impact and in investigating the event, but Confirmit cannot be held accountable for damages resulting from data breaches caused by client. |
**Notification of personal data breach**

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
</table>
| 33   | - processor shall notify the controller without undue delay after becoming aware of a personal data breach  
       - controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent |

We will inform you in accordance with the GDPR requirements. Then, you will need to assess whether you need to inform your supervisory authority. Note that the 72 hours limit is applicable to the data controller, but applies only “where feasible”. The processor requirement is for us to convey the breach to you “without undue delay”.

Confirmit keeps a list of parties to be notified in its CRM system (Salesforce).

---

**Data protection impact assessment - DPIA**

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
</table>

---

**Data Protection Officer (DPO)**

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>37-39</td>
<td>The GDPR requires both controller and processor to have this role in place within their respective organizations whenever personal data is processed. Some exceptions apply.</td>
</tr>
</tbody>
</table>

---

**Transfer of personal data to third countries / cross-border processing**

<table>
<thead>
<tr>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>44</td>
<td>You as the data controller define where in the world you collect the data. The collected data is transferred over the web to, and processed in, the country of the SaaS environment you have selected. Confirmit processes the data in accordance with the data protection laws applicable to the country in which it is being processed by us. Unless you instruct us to do so, Confirmit does not move the data onwards to other countries. Our personnel in our affiliates may however access your personal data in order to provide technical support, management of the SaaS Service, or consulting services. Our affiliates will all comply by the European data protection laws, given all such affiliates have signed our Personal Data Transfer Agreement, built for us by privacy lawyers at Taylor Wessing in the UK and based on the Standard Contractual Clauses (Model Clauses). Further, our US based entity Confirmit Inc. is Privacy Shield certified: <a href="https://www.privacyshield.gov/participant?id=a2zt0000000TNdkAAG&amp;status=Active">https://www.privacyshield.gov/participant?id=a2zt0000000TNdkAAG&amp;status=Active</a>. Finally, we are certified by TrustArc (formerly TrustE) for Enterprise Privacy Certification, see <a href="https://privacy.truste.com/privacy-seal/validation?rid=6f630ece-d54d-4eb1-b869-01d38c78d8b1">https://privacy.truste.com/privacy-seal/validation?rid=6f630ece-d54d-4eb1-b869-01d38c78d8b1</a>.</td>
</tr>
</tbody>
</table>

---

(*) Comment to 28 (g)

The back-ups media is encrypted AES-256 and stored offsite with a specialized third party (Iron Mountain). Iron Mountain does not have access to the encryption key, so the data is irretrievable and without value as long as it remains stored there or elsewhere. After 52-weeks offsite, the back-up media is repurposed for back-ups of the latest data (52-weeks rotation). Only when the back-up tapes are sent back to the data center, would Rackspace, the party holding the encryption key, be able to retrieve data. As it pertains to the GDPR and concepts such as those in articles 16 (rectification), 17 (right to be forgotten) and 18 (restriction of processing), there is no guidance from the European Data Protection Supervisor / Article 29 Working Party in relation to whether those rights also apply to encrypted backups. Accordingly, consensus is that as long as the back-ups are encrypted and the holder of the back-ups does not possess the key, the purposes of the GDPR in relation to data protection are met (encrypted offsite back-ups are blocked from further processing by default). In the event you as our client were to invoke the retrieval of datasets from back-ups, and to the extent you have applied edits to data records on the equivalent datasets stored on the production environment on the basis of data subject requests under the GDPR, you must make sure to apply the same changes also to the data retrieved from back-up.