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 the subject matter. This document must not be interpreted as legal guidance. We recommend that you seek your own legal advice and monitor this field 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.

Starting May 25th, 2018, the Data Protection Directive will be superseded by Regulation (EU) 2016/679 (the "GDPR") applicable to all EEA countries. Please read this for a high level overview. Also, here is the full GDPR text as of April 26th 2016.

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, in a consistent way across the EEA countries. The GDPR provides data subjects with rights in relation to personal data they have shared with businesses and organizations that collect, store, and process such personal data.

Personal Data = more than you may think…

Article 4(1) of the GDPR says:

‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); 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 or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Who does the GDPR apply to?

Every business or organization collecting personal data from “data subjects who are in the Union” (Article 3.2) is subject to the GDPR. A business or organization 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 data subjects who are in the EEA, the GDPR applies to you. Note that “who are in the Union” means data subjects who are in the Union at the time of data collection, and is not related to nationality of the data subject.

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 GDPR 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.

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, who have created the Data Processor Agreement (DPA) we offer our clients to sign with us.

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

Further, as of November 2017, Confirmit has successfully completed the Service Organization Control SOC 2 Type I examination for the Horizons SaaS offering. This comprehensive audit validates Confirmit’s strong commitment to the security, confidentiality and availability of the Horizons SaaS platform. The audit report is made available to our customers upon request.
Some useful sites about data protection and privacy

NOTE: We are providing these links for your convenience. We are however not endorsing the content provided and cannot guarantee accuracy or relevance.

GDPR Full Version

EU Glossary of data protection terms

The “Article 29 Working Party” provides the European Commission with independent advice on data protection matters and helps in the development of harmonized policies for data protection in the EU Member States.

• Guidelines homepage
• Guidelines on Consent

Our UK lawyers at Taylor Wessing offer public access to a wealth of useful data protection information, refer to their Global Data Hub. 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, here.

In the UK, the Information Commissioner’s Officer (ICO) provides ongoing guidance in the data protection area. Although the ICO does not represent other EEA countries, their views are often deemed relevant across countries. Here are a few pieces we recommend:

• Here is a good, relatively short, high level memo from the UK Information Commissioner’s Office (ICO)

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:

• Overview of key items
• Obligations of controllers

Hunton & Williams published a good 30-minutes summary of GDPR on June 19th 2017 here.
APPENDIX 1
Questions & Answers

NOTE: Data controller: you. Data processor: We, 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, see here. 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 early 2018. Article 29 Working Party guidance on consent is published here.

Q: Is consent required for any processing of personal data?
A: No. Consent is only one of six lawful grounds for processing personal data, see Article 6. Two of the other legal grounds are 6.1.(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; and 6.1.(c) processing is necessary for compliance with a legal obligation to which the controller is subject.

As an example, Confirmit needs not obtain consent in order to enter user details in the Horizons software for the purpose of providing services under an agreement with client. Confirmit however needs to obtain consent from data subjects it collects data from as a data controller as part of its marketing and prospecting activities.

Prevailing opinion is that consent is required for data collection via surveys, but your company needs to assess the correct legitimate basis for its processing.
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. See “Personal Data = more than you may think” on page 1 of this memo.

Q: Our company is not collecting any personal data originating from the EEA. Does the GDPR apply to us?
A: No.

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?
A: Yes. See here. The US is deemed to provide adequate protection if the recipient is registered under the US Department of Commerce's US-EU Privacy Shield. Both Confirmit, Inc. in the US and our current provider of data center facilities in the US, Rackspace US, Inc., are listed here.

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. In absence of your Privacy Shield certification they may ask you to sign the EU standard contractual clauses (Model Clauses).

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. Companies like this often use EU standard contractual clauses (Model Clauses).
**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](http://www.rackspace.co.uk/certifications) for the UK and AU, and the Compliance and Validation section of [https://www.rackspace.com/security/global-enterprise](https://www.rackspace.com/security/global-enterprise) 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). Data is retrieved from back-ups only based on clients’ instructions provided to us to via requests sent to our support team. 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 definitive requirement. Data at rest on Horizons SaaS Services will be encrypted by default throughout 2018. Until then, encryption at rest is offered as a chargeable Add-On. For other encryption options, see [this page](#). See also #32 of Appendix 2 for details.
**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, and the audited report of Confirmit’s SOC2 (AT101), 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 SOC 1 ISAE3402 / SSAE 18 (formerly SSAE16), and SOC2 (AT101) Type 1 and Type 2?**

A: As of the fall of 2017 Confirmit has been successfully audited in accordance with SOC 1 and SOC 2, Type I, for security, availability and confidentiality. The auditing is performed by Armanino in the US. We 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.

However, Confirmit has contracted outside legal counsel (Føyen Torkildsen ) to create a GDPR-compliant Data Processor Agreement ("DPA"), relevant to the self-service nature of the SaaS Service. The DPA constitutes an addendum to the current agreement already in place between you and us. Please contact Confirmit and we will sent the DPA to you for your review and signature.

**Q: Does the GDPR require us to sign any agreements directly with Confirmit’s subprocessors?**

A: No. The GDPR does not introduce a requirement for Confirmit’s subprocessors 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 our subprocessors. 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. You may also have authorized other subprocessors via signed schedules or statements of work.

Confirmit remains responsible for the acts and omissions of its subprocessors.
**Q: Who is responsible for initiating the deletion of personal data on the SaaS, when no longer needed?**

A: The data controller is. GDPR Article 1 (e) 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 at your own self-service initiative. Confirmit will in any event 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 Articles 15 to 22 of the GDPR?**

A: No. Articles 15 to 22 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: In relation to requests from data subjects asserting any of their rights under Articles 15 to 22, how quickly am I as the data controller expected to respond?**

A: You have good time, one month, or even more. Article 12 (3) states the following: “The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. The period may be extended by two further months where necessary, taking into account the complexity and number of the requests”. The timelines are not about complying with the request, they are about informing of the progress.

Note that under GDPR Article 12 (4) you may not take action, but you still need to inform the data subject, provide reason, and inform of their possibility of lodging a complaint with a supervisory authority.

**Q: Can I, being the data controller, charge for assistance to data subjects asserting any of their rights under Articles 15 to 22?**

A: Not normally. Article 12 (5) of the GDPR prohibits the data controller from charging a fee for the provision of the personal data, unless the data controller can demonstrate that the requests are manifestly unfounded or excessive, “in particular because of their repetitive character”

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

A: Yes. Complaints can be sent to several actively monitored Confirmit e-mail addresses such as privacy@confirmit.com, abuse@confirmit.com, and dataprotectionofficer@confirmit.com. Further, data subjects may file a complaint in relation to personal data processed on their behalf via the TrustARC’s Privacy Dispute Resolution portal, which is referred to amongst others from Confirmit’s Privacy Policy. 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. The speech was followed up on September 14th 2017 by the Data Protection Bill, published by the U.K. government. Its primary aim is to incorporate the GDPR into UK law and deal with permitted derogations. It aims at providing continuity during and after Brexit and to ‘Brexit proof’ the legislation so that it continues to work in a post-Brexit environment. The Bill is intended to come into force from 25 May 2018, the date from which the GDPR will apply.
## 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. Confirmit is developing features within the Horizons software enabling the ability to assign a retention period to each and one survey database. Confirmit is also developing features enabling transformation of selected data records such that they may be rendered anonymous, and consequently no longer fall under the GDPR requirements, see comment to Article 11 below.</td>
</tr>
<tr>
<td>Consent</td>
<td>6, 7, 13 etc.</td>
<td>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...</td>
<td>Out of all requirements under the GDPR, consent is, in our view, the key one for data controllers to be on top of from day one. Consent is the 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. Guidance on consent was provided by Article29 Working Party in November 2017, see links in page 4 of this memo. If you already have obtained consent and the consent already meets GDPR requirements, GDPR does not require new consent. If you need to collect consent as part of your data collection activities via the SaaS Service, you may create a questionnaire page for that purpose.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Consent question can be built in the start of the survey.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- The data subject’s right to revert consent may be handled by adding an e-mail address the data subject can contact on your end, the GDPR does not</td>
</tr>
</tbody>
</table>
| 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 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.

The data subject’s rights under GDPR Articles such as 16-20 fall away if the data is not identifiable, see wording for Article 11.2 on the left.

11.1: If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

11.2: Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

12(3) The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. Articles 15 to 22 of the GDPR relate to the data subjects rights in relation to access to their data. As per the content of this Appendix 2, the Confirmit Horizons software supports clients in fulfilling their obligations, and the timelines of the GDPR are ample.

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...
<p>| Right to rectification | 16 | ...data subject shall have the right to obtain ... the rectification of inaccurate personal data concerning him or her. | 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. See also the past paragraph in 15.1 above in this table. |
| Right to erasure (Right to be forgotten) | 17 | ...right to obtain ... the erasure of personal data ... without undue delay ... where one of the following grounds applies (several grounds) | 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. See also the past paragraph in 15.1 above in this table. |
| Restriction of processing | 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 | 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). |
| Right to data portability | 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 machine-readable format and have the right to transmit those data to another controller .... | 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 to the rights in Article 17 of the GDPR to have the data deleted. In accordance with Article 12.3 of the GDPR you will need to “provide information on action taken (under Articles 15 to 22)” to the data subject “without undue delay and in any event within one month”. This timeline may be extended by two further months. So it is key to inform the data subject within these timelines, even if the actual activity may take longer. Under Article 12.4 of the GDPR, if you decide not to take action, you still need to inform the data subject, provide |</p>
<table>
<thead>
<tr>
<th>Automated individual decision-making, including profiling</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>Data Protection by design and by default / Data minimization</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>Use by Confirmit of other processors / subprocessors on behalf of data controller</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 at the bottom of this table (*). |
| Appropriate technical measures to | 28 (f), 32 and | 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 |

---

(*): 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
| **Protect personal data / Prior consultation** | 36 | account the nature of processing and the information available to the processor | “prior consultation” is not necessary unless “the processing 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. |
| **Availability of security information, participation to audits and inspections** | 28 (h) | ... (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 | 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. |
| **Instructions from controller that infringe the GDPR or Member State data protection provisions** | 28 (h) | ... with regards to point (h) ... processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions | To the extent Confirmit personnel are involved in executing Client instructions pertaining to 28 (h), Confirmit personnel will inform client about this. However, this requirement does not in any way take away client's responsibility for only providing instructions that are lawful in relation to Confirmit’s processing of client’s personal data. This is also reflected in Article 82. Where client uses the SaaS on self-service basis, Confirmit is in no position to inform you under 28 (h) as the processing is automated and there is no manual involvement. |
| **Record of processing activities** | 30 | ... 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. |
| **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. | 1. **Pseudonymisation.** This is a process our clients are already performing. 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.

2. **Encryption.** Horizons already supports encryption in transit (data imports / exports, SFTP, secure data collection and access to the SaaS) and encryption at rest. Some of these features are offered as add-ons. You can either allow your staff to use these security features at their own discretion, or ask us to enforce on your behalf to all of your users of the SaaS Service. More details [here](#). Data at rest on our Australian Horizons SaaS Service is already encrypted at rest by default. By mid-2018, we will introduce encryption at rest by default on the EURO Horizons SaaS Service, and on the US Horizons SaaS Service. Until then, if you
<table>
<thead>
<tr>
<th><strong>Personal Data Breach</strong></th>
<th>33</th>
<th>...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</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Notification of personal data breach</strong></td>
<td>33</td>
<td>processor shall notify the controller without undue delay after becoming aware of a personal data breach</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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”.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Confirmit keeps a list of parties to be notified in its CRM system (SalesForce).</td>
</tr>
<tr>
<td><strong>Data protection impact assessment - DPIA</strong></td>
<td>35</td>
<td>This is the responsibility of the data controller. Confirmit will reasonably assist. See EU guidance here: DPIA guidance.</td>
</tr>
<tr>
<td><strong>Data Protection Officer (DPO)</strong></td>
<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>
<tr>
<td><strong>Transfer of personal data to third countries / cross-border processing</strong></td>
<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. Finally, we are certified by TrusrArc (formerly TrustE) for Enterprise Privacy Certification.</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). Data is retrieved from back-ups only based on clients’ instructions provided to us to via requests sent to our support team. 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.