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 changing?

Until May 25th, 2018, European Union (the “EU”) data protection was governed by EU Directive 95/46/EC (the “Data Protection Directive”). This Directive also applied 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Starting May 25th, 2018, the Data Protection Directive was superseded by Regulation (EU) 2016/679 (the “GDPR”) applicable to all EEA countries.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 regulate and protect the processing and storage of personal data collected from within the EEA, 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…

Personal data is more than only electronic data records. 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 process personal data obtained 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 Confirmit 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 is GDPR-Ready

Confirmit has been conducting GDPR-Ready initiatives since the fall of 2016. We have taken a number of initiatives to ensure that by the time the GDPR came 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) were fully met. We are following developments closely as more guidance is being published by the European Data Protection Board (formerly Article 29 Working Party) in relation to the GDPR.

We have been mapping the GDPR clauses towards our operations, both in relation to our role as data processor, and that as a data controller. Further, we have been improving the Horizons Software in order to better facilitate your ability to respond to DSAR (Data Subject Access Requests). See Appendix 2 for the full listing.

As it pertains to our data privacy initiatives, Confirmit has in place a Privacy Shield certification via the US Department Of Commerce, and TRUSTé Verified Privacy. As clients of TrustArc (formerly TRUSTé) and members of the IAPP, we obtain ongoing guidance in relation to privacy and 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 created the GDPR compliant Data Processor Agreement (DPA) we offer our clients to sign with us.

Further, in June 2018, Confirmit successfully completed the Service Organization Control SOC 2 Type II examination (SSAE 18 / AT 101) for the Horizons SaaS offering in relation to security, confidentiality and availability. 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 (see link on bottom of the landing page)

EU Glossary of data protection terms

The European Data Protection Board (formerly “Article 29 Working Party”) provides advice on data protection matters and helps in the development of harmonized policies for data protection in the EU Member States.

- EU A29 Guidelines homepage
- EDPB 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 EEA countries, their views are often deemed relevant across countries.
APPENDIX 1
Questions & Answers

NOTE: Data controller: you. Data processor: We, Confirmit.

Q: When did the GDPR come into effect?

Q: Should my company have taken any actions in relation to the GDPR?
A: Yes. All companies handling personal data originating from the EEA, or companies established in the EEA, should by now have prepared and be ready, given that the GDPR does not entail transitional arrangements.

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 (you) is 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.

Confirmit has created a memo about consent, where we share our finding and views on the matter. We are also explaining how you can create your own consent wording and what it should include. You will find our memo at the bottom of this page.

Article 29 Working Party guidance on consent is published here (July 2018).

Q: Is consent required for any processing of personal data?
A: No, not for any, but for surveys it will normally be a requirement. A bit more context: Consent is only one of six lawful grounds for processing personal data, see Article 6 of GDPR. 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 is not required to 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.
For survey-based data collection there is consensus in the industry that consent is required, although your company needs to assess the correct legitimate basis for its processing.

Note that in relation to internal surveys a company runs with its employees, a prevailing interpretation is that consent in such circumstances cannot be deemed to be freely given and therefore would not constitute a valid means.

**Q: What about all the survey data my company collected prior to May 25th 2018. Does the requirement of consent also apply to that?**

If pre-existing data is anonymized (see “break the link” in #5 of Appendix 2), it can be retained and processed indefinitely.

If pre-existing data is identifiable, then it can be processed further assuming such data was originally collected by provision of consent which meets the current Article 13 GDPR requirements. This will often not be the case though, which in turn strictly speaking would require the data to be anonymized, deleted, or consent to be obtained again in accordance with GDPR. Whether or not companies will do that, and whether or not the supervisory authorities will focus on this specific aspect, remains to be seen.

**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 established in the EEA and is not collecting nor processing 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.

---

1. See these two articles from our lawyers at Taylor Wessing: (i) [Practical Considerations](#), and [Lawful Processing in HR](#). From the former: The GDPR recognises that certain relationships do not lend themselves to free choice and control. Recital 43 explains consent cannot be freely given and will not provide a valid legal ground for processing where there is a clear power imbalance between the data subject and the controller. The Article 29 Working Party (WP29) draft guidance on consent highlights an employer/employee relationship as a situation where an imbalance is likely, saying “the WP29 deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees”.
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 European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay. Adequacy talks are ongoing with Japan and South Korea. 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: Not to our understanding. Companies in the US are authorized to process personal data originating from the EEA provided that they comply with the requirements of Articles 45 to 47 of the GDPR (“Transfer of personal data to third countries”). That said, you may experience increasing demand for more thorough data processing agreements between you and your end clients. In absence of your Privacy Shied 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. 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, see in particular Articles 45 to 47.

Q: Where is Horizons data stored?

A: As of April 2018, 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. Additionally, Confirmit offers two Cloud-based sites, one in Canada and one in Hong Kong. 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 reduce internet latency or because of data localization considerations.

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 (PCI DSS), ISO 9001, and is SOC II audited in accordance with SSAE18 / ISAE3402. See here for further details about Rackspace compliance.

Our Horizons Cloud sites leverage the Microsoft Azure cloud offering, with all the industry leading security and privacy solutions offered by them. See here for details.

Q: The GDPR requires personal data to be retained in identifiable form only for as long as required. How long is data stored on the SaaS? When does Confirmit delete our data from the SaaS?

A: Article 5(e) of the GDPR defines that “personal data shall be 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…”

Key point: It is the data controller (our client) that defines the purpose of the processing, and the one who determines how long the retention of the personal data is necessary. Confirmit’s responsibility is to retain the
data on the SaaS in a safe and secure way until (i) client deletes the data; or (ii) the agreement between us and client expires in which case we delete the data.

In relation to (i), clients operating self-service on our SaaS are able to delete data themselves at any time via the user interface. Clients managed fully by Confirmit can request us, in writing, to delete data on their behalf. Horizons offers a “scheduled deletion” feature whereby it is possible to define a retention period for the whole survey database. The data will be deleted from our SaaS environment at that date. Prior to the deletion date, the system will send an email reminding the project owner that the data will be delete. At that point the project owner can decide to change the date or deactivate the deletion in full.

Horizons offers one further option, and it relates to anonymization of the personal data. The feature enables the transformation of selected data record sets in a survey database, such that those selected data sets (eg, name, email, etc) may be rendered anonymous («break the link»), and consequently so that the remainder of the datasets no longer fall under the GDPR requirements. Data rendered anonymous can, under GDPR, be kept indefinitely, but the data may be subject to other laws or data-specific policies (e.g. policies presented to respondents upon the collection) which may still regulate retention. In more details, this feature will first look in respondent data for the fields specified (e.g. email, name), and if found, remove data in those fields and set the values to “null”, and then do the same in response data, if the fields are found there. If a survey is linked to a panel or contact database, the panelid/contactid will also be removed in the survey, (and respid from survey in survey history/survey activity in the count), to prevent joining survey data with personal data in the panel / contact database.

**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 / AU / US sites, Iron Mountain). Data is retrieved from back-ups only based on clients’ instructions provided to us 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 on UK / US, and after 12 weeks offsite on AU, the back-up media is repurposed for back-ups of the latest data (x-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 Board / Article 29 Working Party in relation to whether those rights also apply to encrypted backups. But the ICO provides guidance (see text under the table on the last page of this memo). 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.

Other than in a disaster recovery scenario, Confirmit will only retrieves back-ups upon the written instruction of our client. The recovery is performed on a project-by-project basis.
**Q: Are IP addresses deemed to be Personal Data, and if so does Horizons collect those?**

A: Yes, guidance from authorities points at IP addresses being Personal Data.

In Horizons, IP’s are not stored by default in surveys, however there are script functions that you can use in case you as a client intend to actively collect IPs. If you do so, you will have to follow the rules applicable to you as a data controller, in the same way as for any personal data record you collect.

IP’s are however necessary for security and troubleshooting reasons. Here are more details of how this datatype is managed back-end. Note that IP’s referenced in the following are only available to Confirmit’s SaaS Operations team, not to you as our client.

(i) In order for Confirmit to ensure security, uptime, have sufficient information for possible forensic reviews, and assist with troubleshooting, Horizons stores the respondent’s IP address for each survey page visit, along with the projectid, respid and first qid on the page they visited. We clean out all data older than 31 days on ongoing basis. This log data is backed up to encrypted media on daily basis and is kept in offsite storage for 52 weeks.

(ii) Additionally, we store IIS logs which contain client-IP and projectID (as part of the URL that's logged for each visit) but no reference to the question or to data. We clean out all data older than 35 days on ongoing basis. The IIS log data is backed up to encrypted media on daily basis and is kept in offsite storage for 52 weeks.

In relation to (i) and (ii) above, it is Confirmit’s view that this time limited data retention is both required and necessary for us to meet the requirements of the GDPR in relation to data protection so to reduce likelihood of security breaches. Examples of use we make is to block IPs that are captured by our monitoring systems and deemed to potentially cause a threat to the integrity of the data on the SaaS. For access to a copy of our “SaaS Log Retention Policy” including full details, please contact us

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

A. No. Encryption is one option to be considered under the GDPR, but it is not a requirement. That said, all data stored (“at rest”) on Horizons SaaS sites (UK, US and AU) is encrypted by default. Any personal data Confirmit employees process anywhere other than on the SaaS, is encrypted at rest and in transit.

**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 Type II (SSAE 18 / 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 SOC2 (SSAE 18 / AT101) Type 2?

A: As of the June of 2018 Confirmit has been successfully audited in accordance with SOC 2, Type II, (SSAE18, AT101) for security, availability and confidentiality. The auditing is performed by Armanino in the US. We share the reports with our clients on request. Confirmit intends to have similar audits carried out yearly.

Q: Does the GDPR require us to sign a new agreement with Confirmit, or to enter into separate Data Processing Agreements (DPA)?

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, and in particular meeting the requirements of GDPR Article 28.3.

Confirmit offers its existing SaaS clients to upgrade their current SaaS agreement to GDPR compliance by signing our GDPR-compliant Data Processor Agreement (“DPA”), created by outside counsel to be aligned with the self-service nature of the SaaS Service. The DPA constitutes an addendum to the current SaaS (On-Demand) agreement already in place between you and us. Please contact Confirmit and we will send the DPA to you for your review and signature.

Q: Does the GDPR require Confirmit's clients to sign 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: 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? Also referred to as DSAR = Data Subject Access Requests

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 DSARs under the GDPR, or under any other laws applicable to personal data, we will always confirm receipt of the e-mail to the data subject, and then 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 (DSAR) asserting any of their rights under Articles 15 to 22, how quickly am I as the data controller expected to respond?

A: You have relatively 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. This is outlined in Confirmit’s Privacy Notice, Section 6. Complaints can be sent to several actively monitored Confirmit email 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. 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 EEU but outside of the UK (for example in Germany)?

A. On February 12th 2019 the European Data Protection Board issued a guidance memo in relation to the consequences of a hard-Brexit (a Brexit without a separation agreement with the EU) for transfers of personal data in and out of the UK. Should the UK and EU agree on a separation agreement after all, a transition period through December 31st 2020 would apply and nothing would change for that period i.e. the current GDPR rules for processing (including storage) of personal data originating from within the EEA, shall still apply to processing (including storage) of that data in the UK during that period.

The guidance memo for hard-Brexit makes it clear that even after March 29th 2019 (the “Brexit Date”) the storage and processing in the UK (which at that point will no longer be in the EEA) of EEA personal data is still fully legal and permitted under GDPR. Accordingly, it is not required as a consequence of Brexit (irrespective of whether hard or soft) for Confirmit to set up a SaaS hosting environment in the EEA in addition to the one in the UK. However, depending on the jurisdiction under which you (the Confirmit customer) have entered into an agreement with us, and the jurisdiction of the Confirmit entity with whom you have entered that agreement, we may be required to enter into the EU Standard Contractual Clauses (SCCs / Model Clauses) as explained in the EDPB guidance memo and as summarized below. The SCCs are pre-defined EU approved clauses and are not subject to negotiation, so signature thereof is a lean task.

Here is a simplified summary of the main scenarios, please do contact us at Confirmit if in doubt:
1. If your company’s agreement is with any Confirmit entity other than Confirmit Ltd (UK) nothing changes. Those Confirmit entities are responsible for any onward transfers out of the EU of data under their control, and we are already compliant by means of Confirmit’s intra-group SCC agreement, as well as SCCs signed with Rackspace (hosting environment provider in the UK).

2. If your company’s agreement is in the name of an entity in the EEA but outside of the UK, and entered with Confirmit Ltd (UK), and your data is processed on the SaaS hosting environment in the UK, then, in the event of a hard-Brexit, your company (acting as the data exporter / controller) and Confirmit Ltd (UK) (acting as the data importer / processor) would need to execute the SCCs before the hard-Brexit date.

3. If your company is registered in UK, your agreement is with Confirmit Ltd (UK) and your data is processed on SaaS hosting environment in the UK, nothing changes.

Note – as between Confirmit and you, the SCCs are intended to be entered into between (i) an EEA customer of Confirmit (the data exporter), and (ii) a Confirmit entity (the data importer) outside of the EEA (after Brexit, the UK will be outside the EEA). Further, signature of SCCs are not appropriate where the data importer is in a jurisdiction already approved by the EU Commission under GDPR 45 (“adequacy decision”). The processing of personal data from the EEA on our SaaS servers in the US fall into this latter category and is already covered under Privacy Shield with no need of SCCs.

**Q: Does the GDPR prohibit the sending of personal data via e-mail?**

**A: No.** But the GDPR requirements for considering methods to “ensure a level of security appropriate to the risk” still apply. At Confirmit we have enabled opportunistic TLS for all e-mails we send. And all imports / exports of data Confirmit employees sent to / from the SaaS, are enforced to PGP and / or SFTP.

**Q: Does the GDPR set forth requirements for opt-outs in e-mail correspondence?**

**A: No.** GDPR focuses on lawful basis of processing (Article 6) where consent for the specific data processing initiative is a method widely used. Consent must be specific for the specific processing, not broad, so GDPR itself opens for multiple consents having to be asked, one for each initiative (survey). Opt-Out is different, and GDPR does not require any process for opt-out handling. That said, opt out would be covered by other industry practices (such as ESOMAR) and potential other laws (ePrivacy Directive).
## 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 Horizons platform permits processing of virtually any type of data; customers, employees, suppliers, general market or social research through surveys, web scraping or importing data from other systems via integration or file transfer. The types and categories of data collected are controlled by the data controller (you). Horizons provides options for totally anonymized data collection (for example open surveys or surveys with external respondent generation). For certain types of data collection, personal data will be required, for example to send survey invitations via email or to call a respondent for a phone interview (CATI). The Horizons 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 agreement and with data controller’s instructions. Data controllers can at all times delete records, partial or full datasets from the Horizons software at their own initiative. Horizons offers (<em>) a feature enabling users to assign a retention period to each and one survey database. The data in the survey database will be deleted at the specified date. Prior to the deletion date, the system will send an email reminding the project owner that the data will be deleted. At that point the project owner can decide to change the date or deactivate the deletion in full. For clients on SaaS and Cloud, back-ups available in case the deletion was not intended. Further, Horizons includes (</em>) a feature enabling transformation of selected data record sets in a survey database, such that those selected data sets (eg, name, email, etc) may be rendered anonymous by overriding the data with “null” (“break the link”), and consequently so that the remainder of the datasets no longer fall under the GDPR requirements, see comment to Article 11. Such anonymization can be performed as a “point in time” task, or as a recurring tasks nulling datafields based on record age. In a bit more detail, the “break the link” solution will first look in respondent data for the fields specified (e.g. email, name), and if found, remove data in those fields and set the values to “null”, and then do the same in response data, if the fields are found there. If a survey is linked to a panel or contact database, the panelistid/contactid will also be removed in the</td>
</tr>
</tbody>
</table>
| Consent | 6, 7, 13 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, consent is a fundamental one. Consent is the responsibility of the data controller. Specific requirements are set forth in the GDPR in relation to when consent is required, and the modalities for obtaining a valid consent. Guidance on consent was provided by Article 29 Working Party in November 2017 and adopted in April 2018, 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 establish that you need to collect consent as part of your data collection activities via Horizons, you may create a questionnaire page for that purpose.

- Consent question should be placed at the start of the survey.
- The data subject’s right to revert consent may be handled by adding an email address the data subject can contact on your end, the GDPR does not require “access portals” or similar.
- Horizons 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 Add-On feature.

See Article 13 of the GDPR for “Information to be provided where personal data are collected from the data subject”

There are a number of companies offering comprehensive consent management platforms. In our belief, this level of features is not required in our industry, but each of our clients will need to assess this on their own. A couple of companies we have come across, but have no experience with, are TrustArc and ConsentCheq. |
<p>| Processing which does | 11 | 11.1: If the purposes for which a controller processes personal data do not or do no | A majority of the data analysis and reporting that data controllers carry out in Horizons, does not require personal |
| Right of access by the data subject | Articles 15 to 22 of the GDPR relate to the data subjects rights in relation to access to their data. 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 reason, and inform of their possibility of lodging a complaint with a supervisory authority. |
| 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. As a data controller using the Horizons platform you are able to export, at your self-service initiative, data-files using standard Horizons data export functionality. Exports can be tailored so to only provide responses for specific individuals. This can be done for surveys in production as well as archived surveys. If you anonymize or delete the data as described in “Accountability – 5” above, this whole set of “rights of access” requirement fall away as you will no longer possess personal data. Should you receive requests requiring you to search via many surveys for the existence of data of specific data subjects, this may be a time consuming task. In such case you are welcome to contact Confirmit support for assessing whether we can assist you more efficiently. The approach we recommend is based on the use of the Horizons Application Programming Interfaces (APIs). We have an API Console application developed for internal use, which can export three files per survey project: (i) XML survey definition, (ii) respondent data; and (iii) response data. It is possible to use a filter expression to only retrieve specific records based on fieldname(s) and value(s). The API Console permits exports of multiple projects. |
| not require identification | 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. 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 reason, and inform of their possibility of lodging a complaint with a supervisory authority. |
| 12(3) | 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. As a data controller using the Horizons platform you are able to export, at your self-service initiative, data-files using standard Horizons data export functionality. Exports can be tailored so to only provide responses for specific individuals. This can be done for surveys in production as well as archived surveys. If you anonymize or delete the data as described in “Accountability – 5” above, this whole set of “rights of access” requirement fall away as you will no longer possess personal data. Should you receive requests requiring you to search via many surveys for the existence of data of specific data subjects, this may be a time consuming task. In such case you are welcome to contact Confirmit support for assessing whether we can assist you more efficiently. The approach we recommend is based on the use of the Horizons Application Programming Interfaces (APIs). We have an API Console application developed for internal use, which can export three files per survey project: (i) XML survey definition, (ii) respondent data; and (iii) response data. It is possible to use a filter expression to only retrieve specific records based on fieldname(s) and value(s). The API Console permits exports of multiple projects. |</p>
<table>
<thead>
<tr>
<th><strong>GDPR Memo</strong></th>
<th><strong>Property</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Right to rectification</td>
<td>16</td>
<td>...data subject shall have the right to obtain ... the rectification of inaccurate personal data concerning him or her.</td>
</tr>
<tr>
<td>Right to erasure (Right to be forgotten)</td>
<td>17</td>
<td>...right to obtain ... the erasure of personal data ... without undue delay ... where one of the following grounds applies (several grounds)</td>
</tr>
<tr>
<td>Restriction of processing</td>
<td>18</td>
<td>...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>
</tr>
<tr>
<td>Right to data portability</td>
<td>20</td>
<td>....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 ...</td>
</tr>
<tr>
<td>Automated individual decision-making, including profiling</td>
<td>21+22</td>
<td>Not applicable. Article 71 of the preambles of the GDPR makes it clear that this clause falls outside of the scope of the Horizons software and services Confirmit offers.</td>
</tr>
<tr>
<td>Data Protection by design and by default / Data minimization</td>
<td>25</td>
<td>the controller shall (...) implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization (...)in order to meet the requirements of this Regulation and protect the rights of data subjects</td>
</tr>
</tbody>
</table>

Personal data can easily be edited 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 you anonymize or delete the data as described in “Accountability – 5” above, the “right of rectification” requirement falls away as you will no longer possess personal data.

Horizons enables users, on self-service basis, 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 you anonymize or delete the data as described in “Accountability – 5” above, the “right to be forgotten” requirement falls away as you will no longer possess personal data.

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).

Horizons supports the ability for users to export data-files in a range of different formats using standard data export functionality, which can be filtered to provide only responses from specific individuals.

See also the last paragraph in 15.1 above in this table.

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 to minimize 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 the Horizons software. See here for a **summary page of security**.

Confirmit will support client audits mandated under the GDPR,
<table>
<thead>
<tr>
<th>Use by Confirmit of other processors / subprocessors on behalf of data controller</th>
<th>28.2</th>
<th>The processor shall not engage another processor without prior specific or general written authorization of the controller. In the case of general written authorizations, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deletion and Return of personal data</td>
<td>28 (g)</td>
<td>…at the choice of the controller, (processor) deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies.</td>
</tr>
<tr>
<td>Appropriate technical measures to protect personal data / Prior consultation</td>
<td>28 (f), 32 and 36</td>
<td>…assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor.</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>
</tbody>
</table>

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 of Article 28. Our clients cannot reject to our use of the data center provider (currently Rackspace and / or Microsoft Azure (*), as applicable), as it is an integral part of our offering and we cannot provide the SaaS Service without Rackspace and / or Azure. But we accept responsibility for Rackspace’s and Azure’s acts and omissions, and we warrant compliance to applicable data protection laws on their behalf.

(*) Microsoft Azure is currently only leveraged for the provision of our Cloud sites in Canada and Hong Kong, not for our SaaS sites in Dallas, London and Sydney.

1. Return. Via the Horizons software, 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. Client can also define rules and dates by which data-fields or whole datasets will be programatically deleted, as described in “Accountability – 5” above. 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 (*).

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 by provision of access to applicable documentation (see this security page as a starting point). Be aware however that “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.

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
| 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. Point (h) reads: ...(processor shall) 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. | 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 override client’s own responsibility for only providing instructions that are lawful in relation to Confirmit’s processing of client’s personal data. This is also reflected in GDPR Article 82. Where client uses the SaaS services 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. **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.** Pseudonymisation is easily achieved in Horizons by replacing personal data in a record set with codes. Then, outside of the Horizons SaaS, the list of codes is retained by our client 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 therefore still be linked back to the data subject. According to GDPR, **pseudonymized** data must therefore still be treated as personal data. This is different from anonymized data, where the data subject can never be re-identified. See “break the link” in #5 above. |
| 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 and Cloud Services are 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 | 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 (not Confirmit), 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

This is the responsibility of the data controller. Confirmit will reasonably assist.

Data Protection Officer (DPO)

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. DPO at Confirmit is reachable at dataprotectionofficer@confirmit.com

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

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 or Cloud 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 and Cloud services, 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 (Feb 2018), 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 Verified Privacy.

(*) Comment to 28 (g)

The back-ups media for the Horizons SaaS sites in US, UK and Australia 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 on EURO / US, and 12 weeks off-site for Australia, the back-up media is repurposed for back-ups of the latest data (52/12-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 the data relevant to the request is retrieved. 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 Board / 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.

The above interpretation is consistent with ICO guidance, and was confirmed to Confirmit managers (AF and LD) on call with ICO as of December 2018.