The General Data Protection Regulation ("GDPR"): Consent and Privacy Notice (Policy) in Relation to Use of the Horizons SaaS Software

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 Confirmit’s clients seek their own legal advice.

This document is based on Confirmit’s views of the subject matters herein based on GDPR input from our lawyers, EU authorities, the UK ICO, the European Data Protection Supervisor, WP29, the IAPP, TrustArc, and more.

1. THE GDPR IN SHORT

Until May 25th, 2018, the data protection laws in the European Union (the “EU”) are 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Starting May 25th, 2018, the Data Protection Directive will be superseded by Regulation (EU) 2016/679 (the “GDPR”).

The overall purpose of the GDPR is to protect the personal data, which is the equivalent to personally identifiable information in the United States (the “US”), collected in the EEA. The GDPR provides data subjects with rights in relation to personal data they have shared with companies that collect, store, analyze, and otherwise use personal data ("process").

a. To whom does the GDPR apply?

Every company processing personal data collected from within the EEA is subject to the GDPR. A company does not need to be established in the EEA to be subject to the GDPR. If a company located outside of the EEA processes personal data collected from the EEA, the GDPR applies to that company.

However, the GDPR does not apply if:

1. The company processing the data is located outside of the EEA and is not processing any personal data originating from within the EEA; or
2. The data being processed is anonymous; for example that which cannot be linked back to a data subject.
Note that the GDPR has extended the definition of personal data to include, for example data that together with other data can enable identification of data subjects.

**b. Controllers & processors**

The GDPR discerns between two key roles companies may have:

- 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. Our clients are the data controllers.
  - In some cases our clients may actually be processors themselves because they in turn provide services to a third-party controller. This is the typical case for market research companies. That does however not change the relationship between Confirmit and our client: As between the two of us, our client is the data controller.

- The **data processor** executes the instructions of the data controller either manually or programatically, for example via a software-as-a-service (“SaaS”) offering such as the Horizons SaaS platform. Confirmit is the data processor.

**c. Confirmit’s status in relation to the GDPR**

Confirmit is on schedule to be GDPR-Ready by May 2018. See [https://www.confirmit.com/Legal-Notices/](https://www.confirmit.com/Legal-Notices/), “GDPR – What does it mean for Confirmit’s clients?” Please refer to the Questions and Answers section in Appendix 1 for further information.

**d. Can Confirmit provide legal GDPR advice to its clients?**

It is our clients’ responsibility, not Confirmit’s, to ensure that the surveys and the associated data collection and data processing they initiate and perform are compliant with laws and regulations applicable to our clients. Confirmit cannot interpret the law on our clients’ behalf.

However, we are eager to share our views, and this memo aims at doing that. Please do obtain your own legal guidance.
2. CONSENT: CONDITIONS AND CONTENT

The GDPR requires there to be a lawful basis for processing of personal data. Article 6 of the GDPR sets forth six lawful bases on which a controller can rely. Guidance we have obtained points to consent under Article 6(1)(a) being the only relevant lawful means for data collection via surveys. Note however that in relation to internal surveys a company runs with its employees, there is consensus in the market that consent in such circumstances cannot be deemed to be freely given and therefore not would not constitute a valid means. In such cases one of the other lawful means in Article 6 should constitute the basis of the processing.

a. Consent is the responsibility of Confirmit’s clients in their role as data controllers

Consent is only required when personal data is processed in relation to data subjects within the borders of the EEA at the time of data collection, regardless of the nationality of the data subject. Consent is only required when personal data is processed in relation to data subjects within the borders of the EEA at the time of data collection, regardless of the nationality of the data subject. See here for further details. The best practice is to obtain consent even outside of the EEA because a number of other countries already enacted or plan to enact consent requirements similar to those of the EEA.

In the following we will share our views on the conditions required for consent to be valid, the rules for the information to be provided when consent is obtained ("content"), and then guidelines for you to determine what to include in your company’s consent. In Appendix 1 we share some suggested wording for consent.

b. Conditions of Consent

- Certain conditions for consent have to be met; consent must:
  - be obtained prior to collection or processing of personal data;
  - be prominent, concise, separate from other terms and conditions, and easy to understand;
  - be freely given, specific, informed, and clearly indicative of the data subject’s wishes such as an active opt-in. Pre-ticked boxes or default settings do not constitute consent;
  - not be inferred or cross referenced to URLs in other areas;
  - must be capable of being withdrawn without detriment to the data subject.

- Further,
  - the data controller must upon request be able to demonstrate that it obtained valid consent prior to the relevant processing;
  - the GDPR does not set a specific time limit for consent. However, consent is likely to degrade over time depending on the context. You will need to consider the scope of

1 See Article 6 of the GDPR and the following guidance from Taylor Wessing: “…consent will very rarely be appropriate in an HR context because it is unlikely to be genuinely freely given, and that employers should look to base their processing on the ‘legitimate interests’ justification, or on another ground such as the processing being necessary for performance of a contract or due to a legal requirement.”
the original consent and the individual’s expectations. The best practice, but not a requirement, would be to inform the data subject how long the data will be retained;
  o there is a requirement of keeping records to evidence consent: who, when, how, and what they were told. This is achieved by default if a Horizons questionnaire page is used.

c. Content of Consent

- With regards to the content of the consent, the consent text must at a minimum include the identity of the controller and the purpose of the processing (Recital 42). Further, Article 13 says that “at the time when personal data are obtained”, the controller must “provide the data subject with all of…” the items listed in Article 13 of the GDPR (see below).

- Article 13 does however not say that all the information listed therein has to be included in the consent itself; it says the information must be “provided.” WP29 guidance is that “… not all elements named in Articles 13 … must always be present as a condition for informed consent” as long as a privacy notice is referenced to. WP29 consent guidance from November 2017, page 15, says:

  A controller that relies on consent of the data subject must also deal with the separate information duties laid down in Articles 13 and 14 in order to be compliant with the GDPR. … However, this section is written in the understanding that valid “informed” consent can exist, even when not all elements of Articles 13 and/or 14 are mentioned in the process of obtaining consent (these points should of course be mentioned in other places, such as the privacy notice of a company).

- Accordingly, based on the above, Confirmit’s lawyers’ view is that the content of the consent can be limited to the identity of controller, the purpose of processing, a link to the company’s privacy notice, and, assuming the privacy notice includes all that is required by Article 13, nothing else. However, if any of the requirements in Article 13 are not included in the company’s privacy notice, they need to be added in the text of the consent.

  d. How to determine what consent text your company needs to use

The key question is: how much detail does the consent wording have to include? Our view is that one can keep the consent text short if it includes a link to the privacy notice and such notice includes the information required in accordance with Article 13.

Here is Confirmit’s simplified formula for how Confirmit’s clients can determine what text to include in its consent text:

  1. Review the applicable requirements of GDPR Article 13 (see Appendix 2)

  2. Check your company’s publicly available privacy notice and assess which of the GDPR Article 13 items are already covered there
3. The difference between 1 and 2 is what you need to declare in the consent text, but at a minimum always declare the identity of the data controller and the purposes of the processing together with a link to your company’s privacy notice.

In Horizons, a consent question can easily be built in the start of the survey; see suggested approach in Appendix 1.

Consent is not needed every time:
- Consent may not need to be obtained for every survey an individual completes if the original consent is sufficient to cover more than one survey; for example panelists in market research.
- Where client has already obtained consent prior to GDPR and such consent already meets GDPR requirements. This will not be the case for most clients. In order to be fully compliant, new GDPR consent should be obtained.

3. PRIVACY NOTICE

Your company’s privacy notice plays an important part in relation to consent. To the extent you company’s privacy notice informs the data subject about how your company is processing their personal data, you can keep your consent text shorter.

Confirmit’s clients sometimes ask us to add our privacy notice to their invitation e-mail or to their survey. Adding Confirmit’s privacy notice to a client e-mail or a client survey is incorrect. Confirmit acts as the data processor, not the data controller, in relation to its clients. The privacy notice is a declaration made by the party which initiates, uses, discloses, and manages information it collects, including personal data. The applicable privacy notice must therefore be that of the data controller: our client. The client’s privacy notice should mention Confirmit as the data processor and the locations of processing, but the client’s privacy notice cannot be replaced by Confirmit’s privacy notice.

Confirmit’s privacy notice clearly explains the companies’ roles. Section 5 is about Confirmit’s role as data controller and does not apply to where Confirmit assists a client in their data collection activities. Section 4 addresses Confirmit’s role as a data processor and makes it clear that:

If you seek access to correct, amend, or delete inaccurate personal data, or if you seek to invoke any other rights in respect to the personal data under applicable laws, you should direct your query to Confirmit’s customer as the data controller.

We do however offer the data subject the opportunity to contact us if our client is unresponsive:

If you have reached out to our customer and are not getting a reply, you may approach Confirmit in accordance with section 6 below.
APPENDIX 1
Consent text for surveys

--- CONSENT TEXT IN ACCORDANCE WITH ARTICLE 13 ---

Important – the below text is only intended as a suggestion for a starting point for companies creating their own consent wording. It is aimed at covering all the requirements in GDPR Article 13, and we have mapped our wording towards the applicable requirements like this: {13.x.y}. In our view the following do not apply to surveys: 13.1.d; 13.2.e and 13.2.f. As explained above (see “How to determine what consent text your company need to use?”), items covered in your company’s privacy notice need not be included again in the consent text.

This wording cannot be used as legal guidance. We recommend you seek legal advice.

<If you want to permit respondents not in the EEA to go straight to the survey2:> If you are not responding to this survey from within the European Economic Area (EEA), please go directly to the survey by selecting “skip” below.

<Recommended: If want everyone to provide consent:> At <company name3> we take data privacy seriously. {13.1.a}

- We collect the following types of personal data: <list overall types and categories>. The data we collect will be used for the following purposes <explain in short> {13.1.c}.
- The data will be stored on servers in <country> {13.1.f}, <select an option from the following, or write appropriate alternative text>
  - managed by industry leading providers meeting applicable requirements for data protection. <Add if applicable: More details about the appropriate safeguards are available in the privacy notice, see <link>>.
  - provided by industry leading vendor Confirmit, subject to high security standards {13.1.f: “appropriate safeguards”}. The data center is managed by < Rackspace US / Rackspace UK / Rackspace AU >.
- The data may be accessed, subject to strict confidentiality obligations, by recipients who are employees of <company name> and its affiliated entities {13.1.e}, and by our respective subprocessors. <if relevant: A list of our subprocessors is available in our privacy notice, see below link>.
- The data will be retained in identifiable form for <specify retention period. Alternatively: >
  - The data will be retained for as long as <specify retention criteria> {13.2.a}
- You may withdraw your consent at any time {13.2.c} or send us a request for access, rectification, or erasure of your data {13.2.b}. In order to do so, please <select option>
  - send an e-mail to <client e-mail address> and specify the grounds of your request

---

2 Our lawyers recommend against this, their view is that it would be prudent to obtain consent from everyone, since the concept of informed consent is spreading into may countries of the world

3 In some jurisdictions, such as in the UK, full company address must be provided, either here or as a link.
<if there is a form you ask the data subject to complete in order to handle the data subject access request ("DSAR")>: fill in this form to provide us with the information we need to help you⁴

- For more information about our privacy practices, to file a complaint, and for contact details to our company and our Data Protection Officer, see <add link to Privacy Notice URL> (13.1.b). You may have the right to lodge a complaint with a supervisory authority where applicable. (13.1.d)

--- CONFIRMIT’S TEXT IN ACCORDANCE WITH ARTICLE 13 AND BASED ON INFORMATION PROVIDED IN CONFIRMIT’S PRIVACY NOTICE---

Note – the reason this text is so short compared to the foregoing is that 5.B. of our privacy notice addresses most of the items required under GDPR Article 13.

At Confirmit we take data privacy seriously. The data we collect for this survey will be used for the purposes of <explain in short>. Information we are required to provide to you prior to processing your data as described in the General Data Protection Directive (GDPR) is available to you in Section 5.B. of our privacy notice. For any question related to data privacy, to contact us, or to assert your rights, please see the contact details in Section 6 of our privacy notice.

- I consent and want to move to the survey
- I do not consent and do not want to take the survey

---

⁴ Under the UK Data Protection Act, it is permitted to invite a data subject to complete a form in order for them to present their Subject Access Request ("SAR"); see ICO guidance here. It cannot be the only offered approach. We expect this to be the case also under the GDPR.

⁵ Items included in the privacy notice can replace the items included in the consent text, except the identity of the controller and the purpose of processing.
APPENDIX 2
Key GDPR clauses related to consent

**Conditions for consent:** GDPR Article 7

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

- Consent of minors: See Article 8
- Consent for scientific research: See recital 33 and WP29 consent guidance.

**Consent Requirements:** GDPR Article 13 – “Information to be provided where personal data are collected from the data subject”

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
   a. the identity and the contact details of the controller and, where applicable, of the controller’s representative;
   b. the contact details of the data protection officer, where applicable;
   c. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
   d. where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
   e. the recipients or categories of recipients of the personal data, if any;
   f. where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:
   a. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
b. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

c. where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

d. the right to lodge a complaint with a supervisory authority;

e. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

f. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
APPENDIX 3
WP 29 guidance about consent

This Appendix 3 should be read in context of section 2 above (“Consent”).

Consent is required only when personal data is processed in relation to data subjects. Under the GDPR, a data subject is anyone who is within the borders of the EEA, EEA citizens or not, when their personal data is collected, whose personal data is being processed. They have to be within the EU borders at the time of data collection for them to qualify and therefore have the protection of the GDPR; see here for more details.

In the preliminary guidance on consent from the WP29 on November 2017 (17/EN WP259) the WP29 states the following, provided below in italics small font, which indicates that not all of the above 12 items in Article 13 of the GDPR are required to be included in the consent text all of the time:

WP29 is of the opinion that at least the following information is required for obtaining valid consent:

- the controller’s identity
- the purpose of each of the processing operations for which consent is sought
- what (type of) data will be collected and used
- the existence of the right to withdraw consent
- if the consent relates to transfers, about the possible risks of data transfers to third countries in the absence of an adequacy decision and appropriate safeguards (Article 49 (1a)).

In a case where the consent sought is to be relied upon by multiple (joint) controllers or if the data is to be transferred to or processed by other controllers who wish to rely on the original consent, these organisations should all be named.

- Confirmit’s understanding is that this may be the case in some market research settings.

Processors do not need to be named as part of the consent requirements, although to comply with Articles 13 and 14 of the GDPR, controllers will need to provide a full list of recipients or categories of recipients including processors.

- Confirmit’s understanding is that Confirmit and its subcontractors do not need to be named in the consent. The consent needs to include generic information that processors will be used.

Valid “informed” consent can exist, even when not all elements of Articles 13 and/or 14 are mentioned in the process of obtaining consent (these points should of course be mentioned in other places, such as the privacy notice of a company). WP29 has issued separate guidelines on the requirement of transparency

- This clarification supplements the above short-list compared to the 12 items of Article 13. The requirement of transparency can be met by referring from the consent to client’s information in client’s privacy notice.
Further, from the 17/EN WP259, here are the considerations Confirmit deems to be of key relevance to the type of operations our clients perform on our SaaS platform:

**Legality of processing:** Pursuant to Article 5(1b) of the GDPR, obtaining valid consent is subject to the determination of a specific, explicit, and legitimate purpose for the intended processing activity.

**Granularity:** Consent may cover different operations as long as these operations serve the same purpose. However, a controller that seeks consent for various different purposes should provide a separate opt-in for each purpose to allow users to give specific consent for specific purposes. In such cases the data subjects should be free to choose which purpose they accept rather than having to consent to a bundle of processing purposes. In a given case several consents may be warranted to start offering a service pursuant to the GDPR. If a controller processes data based on consent and wishes to process the data for a new purpose, the controller needs to seek a new consent from the data subject for the new processing purpose. The original consent will never legitimize further or new purposes for processing.

**Informed:** Providing information to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand to what they are agreeing, and for example to exercise their right to withdraw their consent. If the controller does not provide accessible information, user control becomes illusory and the consent will be invalid.

**Prior consent:** Consent should be given prior to the processing activity. In principle it can be sufficient to ask for a data subject’s consent once such as for members of a survey panel. However, controllers do need to obtain a new and specific consent if purposes for data processing change after consent was obtained or if an additional purpose is envisaged.

**How to obtain consent:** The GDPR does not prescribe the form or shape in which information must be provided in order to fulfil the requirement of informed consent. When seeking consent, controllers should ensure that they use clear and plain language in all cases. This means a message should be easily understandable for the average person and not only to lawyers. Controllers cannot use long illegible privacy policies or statements full of legal jargon. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form.

If consent is to be given by **electronic means,** the request must be clear and concise. Layered and granular information can be an appropriate way to deal with the two-fold obligation of being precise and complete on the one hand and understandable on the other hand. To accommodate for small screens or situations with restricted room for information, a layered way of presenting information can be considered where appropriate to avoid excessive disturbance of user experience or product design.

If consent is requested by electronic means, the consent request has to be separate and distinct; it cannot simply be a paragraph within terms and conditions; see Recital 32 of GDPR for further information.

The **use of pre-ticked opt-in boxes is invalid** under the GDPR. Silence or inactivity on the part of the data subject as well as merely proceeding with a service cannot be regarded as an active indication of choice. Blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action to consent.
How to prove consent has been obtained: The GDPR introduces requirements for controllers to make arrangements to ensure they obtain, maintain, and demonstrate valid consent. Controllers are free to develop methods to comply with this provision in a way that is fitting in their daily operations.

It is up to the controller to prove that valid consent was obtained from the data subject. The GDPR does not prescribe exactly how this must be done. The controller may keep a record of consent statements received so they can show how consent was obtained, when consent was obtained, and the information provided to the data subject at the time. The controller must be able to prove that a data subject in a given case has consented. As long as a data processing activity lasts, the obligation to demonstrate consent exists. After the processing activity ends, proof of consent should be kept no longer then strictly necessary for compliance with a legal obligation or for the establishment, exercise, or defense of legal claims in accordance with Articles 17(3b) and 17(3e) of the GDPR.

How long does consent last: There is no specific time limit in the GDPR for how long consent will last. How long consent lasts will depend on the context, the scope of the original consent, and the expectations of the data subject. If the processing operations change or evolve considerably then the original consent is no longer valid. If this is the case, new consent needs to be obtained.

WP29 recommends as a best practice that consent should be refreshed at appropriate intervals.

Withdrawal of consent: Withdrawal of consent is given a prominent place in the GDPR. The GDPR does not say that giving and withdrawing consent must always be done through the same action. However, when consent is obtained via electronic means through only one mouse click, swipe, or keystroke, data subjects must in practice be able to withdraw that consent equally as easily. Where consent is obtained through use of a service-specific user interface, for example via a website, app, log-on account, interface of an Internet of Things device, or by e-mail, a data subject must be able to withdraw consent via the same electronic interface as switching to another interface for the sole reason of withdrawing consent would require undue effort.

The above paragraph makes sense for situations where a data subject visits a site and provide consent (eg marketing). It does however not make much sense in the setting of surveys. Our lawyers agree that withdrawal of consent for processing of data in relation to surveys, may be better offered via an a-mail request or a short pre-defined form.

All data processing operations that were based on consent, took place before the withdrawal of consent, and were performed in accordance with the GDPR remain lawful; However, the controller must stop the processing actions concerned when the data subject withdraws consent. If there is no other lawful basis justifying the processing, for example further storage, of the data, the data should be deleted or anonymized by the controller.