Let's go further

FAQ – EG and data security

Version 4
10.06.2020

Questions	Answers
What are EG's responsibilities as a data processor?	As a data processor, EG must act exclusively according to the customer's instructions. This means that EG processes personal data on behalf of the customer. EG does not decide how or for what purpose personal data is processed. EG is, therefore, responsible for following the customer's instructions and helping the customer fulfil their obligations under GDPR. EG shall comply with the data processing agreement it has entered into with the customer. The data processing agreement covers EG's responsibilities in more detail.
What is the customer's responsibility in the cooperation with EG?	In general, the customer is responsible for ensuring that processing of collected personal data complies with GDPR rules. As data controller, the customer must ensure that the customer 1) is permitted to process the data that you and your data processors are in possession of 2) has a data processing agreement that meets the requirements of the GDPR 3) performs inspections of your data processors 4) reports any breaches to the Danish Data Protection Agency within 72 hours 5) can document to the Danish Data Protection Agency that you have secure data protection with the appropriate technical and organisational measures to prevent unintentional, unreasonable or illegal processing.

What is a data processing agreement?	A data processing agreement is a legally binding document between the customer and EG. The GDPR requires that the parties sign such a contract, which contains certain minimum requirements. The data processing agreement stipulates the rights and obligations that apply when EG processes personal data on behalf of the customer.
What is GDPR?	The EU's GDPR is a regulation to strengthen and harmonise the protection of personal data in the EU. A regulation comes into force immediately in each member state, and each member state must orient their own legislation in accordance with the regulation.
Which authority regulates personal data protection in Denmark, Norway and Sweden	Denmark: The Danish Data Protection Agency - https://www.datatilsynet.dk/ Norway: The Norwegian Data Protection Authority - https://www.datatilsynet.no/en/ Sweden: The Swedish Data Protection Authority - https://www.datainspektionen.se/
Where can I read more about the GDPR rules?	You can read more about the GDPR rules on the website of each country's authority responsible for data protection, for example, for the Danish Data Protection Agency, visit https://www.datatilsynet.dk/. You can also visit the European Commission's website here: https://ec.europa.eu/info/law/law-topic/data-protection_da
Why is EG's standard data processing agreement based on the provisions of the Danish Data Protection Agency's standard contract?	The Danish Data Protection Agency has prepared a set of standard contract provisions that is approved by the Council of Europe Data Protection Commission. EG wants to use the Danish Data Protection Agency's standard contract provisions because the Council of Europe Data Protection Commission has determined that the agreement complies with the minimum requires of the General Data Protection Regulation (GDPR).

Why does EG have several different data processing agreements?	EG has different data processors because EG supplies a range of different services. It is important that a data processor bases its processing specifically on the delivered service because it has n impact on the purpose of processing the personal data concerned.
What is DocuSign?	DocuSign is third party software that EG will be using as its Contract Management system. EG uses this solution to send and receive agreements and documents that need to be signed by the customer. The solution supports a complete digital flow with the option to follow up, save and find important documents. Read more about DocuSign https://www.docusign.co.uk/
How to sign using DocuSign	A guide has been made to explain how to read and approve a document in DocuSign. Read the document here: https://eg.dk/siteassets/media/files/about-eg/guide-til-docusign.pdf
Why does the customer receive more than one data processing agreement from EG?	If EG provides you with more than one service and/or you have entered into various different delivery agreements with EG, there will be a difference in terms of the content. It is imperative that a data processing agreement governs a specific service.
Why do you need to sign a data protection agreement?	As data controller, it is compulsory to enter into a data processing agreement. This means that a data processing agreement must be signed when you use a provider to process personal data on your behalf.
How often does EG update the details on, for example, new data subprocessor agreements?	Data processing agreements are updated regularly.
What happens if as a customer you do not sign the agreement?	If you do not sign a data processing agreement, EG will not be able to process personal data on your behalf.
How can I as a customer be certain that EG looks after my data?	EG has just implemented the technical and organisational measures that ensure a level of security in line with the risks associated with processing of personal data for the specific solution.

How am I as the customer notified if there is a security breach involving my data?	EG follows a fixed defined standard procedure in cases of security breaches. The procedure ensures that the customer is informed as fast as possible when EG becomes aware of a security breach. EG assists the customer with the necessary information making it possible to deal with how it should be reported to the Danish Data Protection Agency. The procedure is approved by our external auditors and is continuously assessed and updated.
What do I do if I am notified that there has been a security breach involving customer data?	As a general rule, all personal data security breaches must be reported to the Danish Data Protection Agency without undue delay and within 72 hours of the data controller becoming aware of the breach. It is only when it is unlikely that the personal data breach involves a risk to the rights and freedoms of natural persons that it does not have to be reported. Refer to the guidelines of the Danish Data Protection Agency: https://www.datatilsynet.dk/media/6558/haandtering-af-brud-paa-persondatasikkerheden.pdf
How does EG define personal data?	Personal data is any form of information that can be referred back to a specific person, even if that person can only be identified by that information being combined with other information.
What type of data does EG store about its customers?	It varies from customer to customer what type of data EG stores for its customers. It depends on EG's instructions and what type of service the customer receives from EG.
How can you see the data EG stores about the customer?	EG processes and stores only the data that you as the data controller instructs and forwards to EG.

Does EG transfer data to countries outside the EU that do not follow the European GDPR?	EG may, in the processing of personal data, transfer data to countries outside the EU/EEA. If EG transfers personal data to the majority of countries outside the EU, the transfer of your personal data to these countries outside of the EU/EEA will be based on the standard transfer contracts drawn up by the European Commission or another similar transfer basis specifically designed to ensure an adequate level of protection. You can read more about the transfer of personal data to countries outside the EU/EEA on the European Commission's website.
Who are the data subprocessors that EG uses?	The individual data processing agreement will state which data subprocessors EG uses for the solution.
Who is EG's DPO (data protection officer)?	If you have any questions about our processing of your personal data, please contact EG's Data Protection Office here: Data Protection Office Industrivej Syd 13 C 7400 Herning, Denmark e-mail: dpo@eg.dk Telephone: +45 7013 2211
Should I have a DPO?	If you are *public authority or organisation* you must always have a data protection officer (DPO). If you are a *private enterprise*, you must have a DPO if: 1) your core activities involve the processing of sensitive data or information on criminal offences 2) to a large extent and 3) the processing activity involves regular and systematic monitoring of persons to a large extent. The duty of private enterprises to designate a data protection officer applies to both the data controller and the data processor. This means that most private enterprises in Denmark that perform "general" processing of personal data, including administration of HR information, customer information, online booking systems, etc. are not obligated to designate a data protection officer. Read more about this in the Danish Data Protection Agency's guide on data protection officers. https://www.datatilsynet.dk/media/6561/databeskyttelsesraadgivere.pdf

Who should I contact at EG if I have questions about our data processing agreement?	If you have questions concerning your data processing agreement, please email agreement@eg.dk
Where can I read about how EG handles personal data?	To find out how EG handles your data, please visit out website https://eg.dk/om-eg/compliance/.
Who do I contact if I find that EG has violated the data processing agreement?	It is in the interests of all parties to comply with the data processing agreement. If you feel that EG has violated the data processing agreement you should contact and make EG aware of this. A violation may involve a misunderstanding between the parties and must be corrected. If a violation has resulted in a breach in data security, you as the data controller are responsible for reporting the breach to the Danish Data Protection Agency within 72 hours.