THE EUROPEAN GDPR EXPLAINED

Stroop!

International

Business Consultants

What is the GDPR?

GDPR stands for “General Data Protection Regulation” and the full title is:

“Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)”

As the title suggests, it is an European regulation for (the processing of) personal data of natural persons. Natural person means a person of flesh and blood. Data of for example limited companies and trusts are not bound by the regulation.

The GDPR came into effect on 25 May 2018 and supersedes all national laws and regulations the EU countries may have had.

In our society personal data is being collected and processed and that is unavoidable. The GDPR was brought to live to protect citizens against wrongful collection and use of their personal data.

Accountability

The GDPR wants companies to think and to consider the data they collect from and process for their customers. It therefore does not present a list of do's and dont's, but it rather tells companies what they have to do to be accountable for their actions.

Each EU country has its own organisation (called the 'supervisory authority') that will have the authority to check if you are accountable. When asked by such an authority, it is your responsibility to not only show how you protect your customer's data, but also what system you have in place to continously do so.

Stroop!
International
Business Consultants

Lawfulness of processing

When are you allowed to process data?

You may only process data when you have legal grounds to do so. It is called ‘lawfulness of processing’. Three types of personal data are distinguished by the GDPR: ‘regular’ personal data, ‘special’ personal data and personal data ‘relating to criminal convictions and offences’.

Regular Personal Data

There are six grounds on which you may process regular personal data: after consent of the person involved, for the performance of a contract, to comply with legal obligations, to protect vital interests of the person or people involved, when needed in the public interest or in exercise of official authority and when processing is necessary for the purpose of legitimate interests except when overridden by the rights and freedom of the person or people involved.

Stroop!
International
Business Consultants

Lawfulness of processing

Special Personal Data

Personal data falls into the category ‘special’ when it reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

It is prohibited to process this kind of data unless one of the following ten exceptions apply:

- You have explicit consent, unless the EU member state where the person lives prohibits an exception based on consent
- You are authorised to do so by law or regulation
- It is neccesary to process the data to protect the person involved and this person can’t give consent
- When it concerns personal data that has been made public by the person him- or herself
- When needed for legal procedures
- When needed for public interest, but only so in accordance with the laws of the each individual EU country
- When needed for medical reasons, but only so in accordance with he laws of each individual EU country and with additional safeguards
- When needed for public health issues, but only so in accordance with the laws of the each individual EU country
- When needed for archiving purposes in the public interest or for scientific or historical research, but only with the proper safeguards in place
- When you are a not-for-profit organisation with a political, philosophical, religious or trade union aim and you process only data of your members and do not share it outside your organisation

Stroop!
International
Business Consultants

Lawfulness of processing

Personal Data relating to criminal convictions and offences

This personal data may only be collected and processed under supervision or guidance of local government. Registries of criminal convictions may only be held under supervision of local government.

Stroop!
International
Business Consultants

Data protection officer (DPO)

The Data Protection Officer (DPO) is someone within your organization who supervises your adherence to the GDPR. The DPO is not responsible though!

There currently (February 2019) are three situations where you have to have a DPO:

- With government bodies and public institutions
- With organisations who have observation of people as their core-business
- With organisations whose core-business it is to process special personal data

Even when you are not obliged to appoint a DPO, you still are free to do so.

Stroop!
International
Business Consultants

Rights of the data subject

The GDPR gives extensive rights to EU citizens (the ‘data subject’) in regards to their personal data. Transparency and modalities are the key words.

This is translated into the ‘right of access’ any person has (someone has the right to know what information was obtained about him/her and who it was shared with), the ‘right to rectification’ of the personal data, the ‘right to be forgotten’ (request to erase all personal data), the ‘right of data portability’ (where you deliver the data you hold in an open format, so the person can take the data to another company) an the ‘right to object’ against processing of their data.

Security and data breaches

Article 32 of the GDPR requires you to secure your processing of personal data. This security must prevent unauthorised access to this data. Should an unauthorised person access the personal data, or even when you don't know if that happened but you can't rule it out, then you have a security breach.

A security breach also constitutes of the situation where you lose personal data (because of a server malfunction for example) and you are not able to restore that data.

In case of a security breach you need, article 55 of the GDPR requires you to inform the supervisory authorities of the countries that were involved in the breach. You need to do so within 72 hours, or when you inform later you need to include your reasons for that. When the breach is likely to pose a high risk to the rights and freedom of the persons involved, you need to inform them as well. When the breach is unlikely to cause a risk to the rights and freedom of the persons involved, you do not have to inform both the supervisory authorities and the persons involved.

Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment (DPIA) is a tool for your company's risk management. The purpose of a DPIA is to consider various incidents that could happen in or to your company, and think of possible solutions. For example, your office gets destroyed in a fire. Are you able to continue with your orders, do you have other computers you and your staff can work from, are you able to redirect your office phone number to a mobile phone?

The GDPR requires companies to do a DPIA in three situations: if you extensively and systematically evaluate personal data, if you extensively process specific personal data or if you extensively and systematically monitor public areas.

The majority of people reading this document will not be involved in the above situations. Nevertheless, it is always good to prepare yourself for "what-if" scenarios. Making a DPIA for your company could benefit you when you need it.

Required documents: Privacy statement

Privacy Statement (art. 13 GDPR)

Your privacy statement informs your (potential) customers about what data you process about them, what you us it for, how long you store it and for what purpose, who you share it with and how they can collect this data from you.

Apart from the above, you also use your privacy statement to inform your customers about their rights and how they can exercise them, such as how they can access the data you hold on them, how they can have data rectified or deleted, but also that they have the right to file a complaint with their national supervisory authority.

For those who are interested, article 13 is copied onto the next page.

Everything you need in your privacy statement is listed in article 13 of the GDPR. This article is quite long and not very easy to read. Stroop! IBC therefore made sure that you can download a privacy statement from their website that is up to code.

Stroop!
International
Business Consultants

Required documents: Privacy statement

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; L 119/40 EN Official Journal of the European Union 4.5.2016 (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. 3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2. 4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Stroop!
International
Business Consultants

Required documents: Records of processing activities

Records of processing activities (art. 30 GDPR)

The record of processing activities must show all categories of personal data that your company processes, the reasons why it processes that data and with whom that data is shared.

This record is not supposed to be a log of your daily activities, but it should be an overview of your company processes in which personal data is being processed.

There is an exemption to having to keep records of processing activities, but unless you process personal data occasionally, you do not qualify for that exempt (when the purpose of your business is to sell products and you make B2C sales, the processing of personal data on those orders cannot be called occasionally).

Stroop! IBC can provide you with an Excel template that helps you to make those records swiftly.

Stroop!
International
Business Consultants

Required documents: Data Processing Agreement (DPA)

Data Processing Agreement (art. 28 GDPR)

When your company outsources work to a third party and this third party handles your customer's personal data, they become your 'processor'. In this scenario you become the 'controller'.

As controller it is your responsibility that the processor handles the personal data according to the GDPR. It is also required that you make clear agreements about this with your processor and that you put this in writing.

The key components of the DPA are that the processor only processes the personal data that you ask them to process, that they may not outsource it to another party without your explicit consent, that they have an obligation to assist you in case of a data breach of investigation on who will bear the cost of such investigations and what happens to the personal data when the cooperation ends. Examples of processors are your bookkeeper and your order fulfillment center.

Stroop! IBC has a template DPA available for download which contains all legal necessities and which only needs to be filled with the company information of your and your controller's companies.

Stroop!
International
Business Consultants

Stroop! GDPR Toolkit

Your company needs to adhere to the GDPR when it processes the personal data of EU citizens. This means that any company worldwide that sells products to B2C customers in Europe, needs to comply with the requirements set out in the GDPR.

The difficulty with the GDPR is that it tells you what you need to do and what you need to have in place, but not how you should do that and how the required documents should look.

To help you become compliant, we made a GDPR Toolkit for you. This toolkit contains all the documents you need to have in place and includes clear instructions on how to personalise them for your company. This toolkit combined with about three hours of your time will make your company GDPR proof. The price for the GDPR toolkit is a modest 55 euro and is available for online download here: https://stroopibc.com/product/gdpr-toolkit/.

Stroop!
International
Business Consultants

Stroop! IBC supports entrepreneurs worldwide to do business in Europe and offers a one-stop-shop solution for logistics, import into the European Union, warehousing and fulfilment of customer orders. They also provide local office addresses, act as a proxy with banks and government agencies on the entrepreneur's behalf and handles European bookkeeping and tax filings.

With offices in The Netherlands and Japan, Stroop! IBC is availabe around the clock and offers you the best of multiple worlds.

Stroop! International Business Consultants B.V.
Laan van Vollenhove 883
3706 ED Zeist
The Netherlands

www.stroopibc.com
info@stroopibc.com

Tel NL: +31 (0)85 888 1447
Tel JP: +81 (0)50 5865 3098

Stroop!
Internationol
Business Consultants