On May 25, 2018, the Data Protection Ordinance enters into force, which places more demands on how we as a company handle personal data in our work. In order to meet the changes, Brief has worked on the following documents with the most important changes and a new way of working.

Table of Contents

Data protection Regulation 2
Information 2
Personal data 2
Sensitive personal data 2
Treatment 2
Responsibility of business 2
Thinning 2
Corrigendum 3
Deletion 3
The Register 3
Security by default 3
The Abuse rule (Email and current text) 3
Right to process the data 4
Personal Data Assistants 4
Privacy Incident 4
Collection of Consent 5
Information is not displayed 5
Appendix 1, Routine for Consent Collection 6
Appendix 2, Personal Data Incident Routine 7

Data Protection Regulation
A new EU law replacing the Personal Data Act (PuL) for handling personal data processing. The regulation is the same throughout the EU, which makes it easier to work with personal data between European countries, and it also places higher security and information requirements than PuL on companies and organizations that process personal data. The Data Protection Ordinance focuses on the data subjects' rights to their tasks, and therefore attaches great importance to these rights and the accompanying obligations that the data processing companies have.

Information

Personal data
A personal statement is a task that alone or together with other information can be used by someone to identify a living person. Company information is therefore not included.
Examples of personal data are: Person ID, Address, Email, Phone Number, Property Identification, Membership Number / Customer Number, Registration Number, IP Address, and Photos of Individuals.
All information that alone or together with other information can be used to identify a person is a personal data. This means that, as a company that processes data, we must also secure information that alone can not identify a person but which in combination with one or more other data could do so.

Sensitive personal data
Certain categories of personal data have been deemed to be so sensitive that they can only be processed if there is direct support in law or the registrant has given their explicit permission. In addition, if treatment is allowed, extra security must be taken into account and the integrity of the registered person.
These tasks are: ethnic origin, political opinions, religious or philosophical beliefs, union membership, genetic or biometric information, health or sexual orientation.
This means that it is very important when registering new notes, changing saved notes or data to verify that they do not contain any sensitive personal data that we do not have legal permission to process. Only if it is really justified can such a task be saved in the computer system. If a customer writes or submits material containing, for example, health information and is not absolutely necessary for the performance of our assignment, such information shall not be saved but deleted after any other information noted in the computer system.

Treatment
When Brief does something with a personal statement, it is called to process the task. When a task is processed, it must be done safely and with the protection of the integrity of the personal task. A treatment is not only when we record information or change it, but also when we store it, when we first register the data in the system or backup the database that is also processing data.

Briefs Responsibility
Responsibility for the correct processing of the data is the sole responsibility of the entire company with the CEO and the Board to be held accountable.

Thinning
Brief may not have data in their computer systems that we do not need. "Good to have" tasks can not be saved just because they are good to have. It is therefore important not to save personal information in email or elsewhere than it should be. For the completion of the assignment to the municipality, data may be required to be saved. The municipality instructs Brief to store information in the control book.

Corrigendum

A person registered in any of Briefs computer systems is entitled to have their duties corrected if they are incorrect. This means that when a registered person contacts Brief and states that the information is incorrect, we must investigate if the information the registrant thinks is incorrect actually. For example, we can do this by comparing the information with the public records or other sources and see if it is consistent. If it turns out that the information we have registered is incorrect, we must correct it as soon as possible.
We must always investigate if the information is correct but need not change if it appears that the information provided by the registrant does not match what we know or can see in public records. Therefore, a customer can not force us to register a new address if we consider that the new address is incorrect.

Deletion

A person registered in any of Briefs computer systems is entitled to have their data deleted if there is no longer any need for the data to be left. The registered person must then contact Brief and announce that it wants us to remove all information about the person in our computer systems. When a registrar requests to be deleted, we need to ascertain as soon as possible if the data is to be deleted. If we find that we do not need the information anymore, they will be deleted without delay. If the investigation shows that we still need the data, for example, if it is required to have a proper control book, then the data will not be deleted.

The Register

A person who is registered in any of the Briefs computer systems is entitled to get an extract from the computer system with all that is registered about the person. The registry extract is free of charge for the registered person and either published electronically or physically, depending on what the registered person wishes. If the person requests multiple registry extracts in a timely manner, Brief is entitled to make a refund for disclosing the material or, in some cases, refusing to provide the information. Refusing such a request, however, requires that we really can state that it is not reasonable to disclose the information, so the main rule is that we will hand out the requested material.

Security by default

The Data Protection Ordinance requires computer systems where personal data are processed to provide security, not only purely technical but also physical security in the premises and procedures for how we work with personal data in the system.
This means, among other things, that we have limitations on how users are entitled to use the systems.

The abuse rule (Email and current text)

Previously, current text in, for example, word documents or mail in the mail program has been excluded from the privacy rules, as long as the treatment has not been violated or misused (hence the name of the abuse rule).
This exception disappears when the Data Protection Regulation is introduced, which means that personal data contained in such programs must now be treated with the same security and privacy as other computer systems. Therefore, we still receive e-mail and write personal data in Excel and Word, but they must be treated in the same safe and legal manner as any other personal data processing.

Right to process the data

In order to process the data, Brief must have a legal basis that allows us to process the data. The legal bases are listed in the Data Protection Ordinance and no other than those expressly written there are allowed.

The grounds that may be relevant to Brief are:

- Consent from the registered
- The treatment is necessary to fulfill an agreement
- There are legal requirements or government decisions that require processing of the data
- The business has a legitimate interest in processing data

Contact information for persons working with customers or suppliers is also personal data and must be treated as such. For the processing of such information, Brief has what is called a legitimate interest in processing the data. In each new such treatment, we assess whether we are more interested in retaining the data than the registrant has in removing it.
Other tasks in our systems may have a different reason and if a registrant contacts us with questions regarding rights and obligations under the Data Protection Ordinance, the person will be referred to the data protection officer on Brief.

Personal Data Assistants

The operations make use of subcontractors to various things in Brief, such as developers and consultants. These subcontractors often handle personal data that Brief has collected and thus also be responsible for. The business has signed a personal data grant agreement with all personal information assistants.

Privacy Incident

A personal data incident is when personal data is accidentally or illegally destroyed, lost, altered, spread or otherwise treated in a way that could harm or violate the data subject.

Examples of personal incidents are:

- Someone steals a computer where personal data is stored
- Someone loses their mobile phone that is connected to the job mail and contains saved files with personal data.
- One or more computers get their hard drives encrypted by a virus

Note that the list is not exhaustive and that more situations can qualify as personal data incidents.

Information need not be stolen or unauthorized

An assignment need not be stolen or sent to an unauthorized person to be considered an incident. For example, it appears that data is destroyed despite the fact that they should be saved to qualify as an incident.

If something has happened to data registered with Brief as it was not thought that it would happen, it could be a personal data incident. Therefore contact the person responsible for data protection issues, to check for a situation where personal data are exposed to risk.

Some incidents need to be reported to the authorities

All personal incidents must be registered in Brief's own incident register, but more serious incidents must also be reported. In case of particularly serious incidents, the registered as a victim must also be informed.

A serious personal data incident must be reported to the Privacy Authority (Data Inspection) within 72 hours of Brief becoming aware of the incident. The report is standardized, a template for reporting personal data incidents has been developed and is in charge of data protection issues at Brief.

If personal information is sent incorrectly, disappears, changes without law or the like

Immediately contact the IT manager or responsible for data management issues as soon as the error is detected. It is very important that responsible personnel receive the information as early as possible as the deadline for reporting an incident is short and begins to run immediately when it is detected, regardless of who detects it.

We collect as much information as possible about what happened but does not change or delete anything before responsible personnel can begin the investigation.

Collection of consent

In some situations, Brief should collect consent from the data subject to process certain tasks. An example of this is whether a representative of a company belongs to and wants to have an invoice sent to its private address or when a person wants us to note sensitive information such as health and disease states.

Information is not displayed

Disposal of personal data may occur after the information is out of date, when our right to process the data is terminated or on behalf of the municipality. After the information has been deleted, nothing remains, so it is not possible to reproduce the information afterwards.

Appendix 1, Routine for Consent Collection

2018-05-25, version 1

1. Verify the person's identity.

2. Inform about our contact information:

2.1. The business processes your personal data in accordance with the Data Protection Ordinance. For contact with the Business, you can either email hello@letsbrief.com or visit our website www.letsbrief.com

3. Inform the terms of the consent.

3.1 Your information will be processed to be able to deliver the work you signed us up for, we process your information with your consent.

3.2 The activities and our personal information assistants, such as helping us print invoices, may be able to share your information.

3.3 The data will be saved as long as they are required to meet the purpose or until your consent is revoked.

3.4 You have as registered the right to request rectification, deletion and limitation of processing of your data, please contact us in such case.

3.5 You may at any time withdraw your consent, then contact us and notify.

4.Inform that the registrant is entitled to complain to the Privacy Authority.

4.1 If you are not satisfied with the information or how we processed your data under the Data Protection Ordinance, you are entitled to lodge a complaint with the Privacy Authority.

5. Note that the registrant consented to personal data processing as well as informed about his rights according to the routine.

Appendix 2, Personal Data Incident Routine

When you discover an event that may be a personal data incident, it is important that you document all the information you may have in the matter.
For example, calling a debtor telling you that he or she has received another person's collection fee in the mailbox, your computer is locked by a virus or accidentally mailed personal information to someone who does not have access to them, so you need to record everything you can about incident and then contact the responsible personnel. Therefore, note the names and phone numbers of them in the box to the right.
Responsible personnel then investigate the incident and then take the necessary measures needed to assess the circumstances and seriousness of the case. You may need to be helpful during the investigation.