GDPR info

GDPR POLICY Handling personal information. This day, 7 May 2018, the following policy has been established for the companies within the My First Home Group, including MFH Bygg AB and the Junior Living companies.

Purpose

We aim to protect the integrity of our clients, employees and partners. They should be able to feel safe about entrusting us with their personal information. Therefore, we have established this policy. It is based on the current Data Protection Laws and clarifies how we work to protect the integrity and rights of our employees, clients and buyers.

The purpose of this policy is to map how we process personal information, what we use it for, who may take part of it and under which circumstances, and how the respective party can make use of their rights. The company has no more than 250 employees and does not need to keep a register nor appoint a Data Protection Officer.

Background

We process personal information foremost to fulfil our obligations, i.e. with legal right and to fulfil legal requirements. Our starting point is not to process more personal information than is needed for the purpose, and we always strive to use the least privacy sensitive information.

At some time, we have used personal information in the form of e-mail addresses to send information. We have also obtained personal information during recruitment processes. Finally, we many times obtain personal information from people wanting to sign up for our apartments.

Clients and stakeholders have the right to object to us using personal information for the purpose of direct marketing. We will only send e-mails with information pertaining apartment projects. The mailings will contain information on how to unregister and be removed from the stakeholder register. MFH Bygg AB/Junior Living, Hufvudsta Gård, Brännеriet, 17173 Solna info@juniorliving.se

Guide Lines

What sort of personal information do we process? We only process personal information when we have the legal right. We do not process personal information in any other case than what is necessary to fulfil our requirements under law and contracts. Here are some examples of the personal information we process:

- Personal information in connection with salary
- Personal information about employees and relations
- Personal information in connection with recruitment processes
- Personal information about the owners and management for our clients
- Personal information about buyers of apartments
- Personal information to be able to handle warrantable issues
- Personal information to keep a register of stakeholders updated.

As much as possible, we try to obtain consent before processing any personal information. The respective party agrees to processing by accepting our general terms and conditions. When they consent to our general terms and conditions, they also consent to us processing their personal information.

The respective party can at any time revoke their consent. We will then no longer process the personal information or obtain new information, provided that it is not necessary to fulfil our obligations under a contract or law.

The company stores data foremost on the server, but information is also saved in physical folders. Server, mobile phone and laptop must be password protected. The company's policy is that e-mail may be used in private context and when an employee leaves, the employee may only delete personal e-mails, not e-mails pertaining to construction projects. Personal e-mails must be deleted as soon as there is no objective reason for not deleting the information, at the latest after 12 months. Documentation regarding projects must be

saved as long as the project guarantee is valid.
When a position is filled, the CV:s of the other applicants must be deleted, unless consent is obtained from them to save the information. All information about employees are saved in the payroll system and the payroll folder, which also includes assessments, concluded training courses etc. Information about employees are not saved anywhere else.

Data Protection Officer

The Data Protection Officer is according to the GDPR as a starting point obligated to inform the registered persons that their personal information is being processed. Information about the handling of personal information must be given out by the Data Protection Officer at the time when the personal information is gathered and also when the registered person asks for it. Regarding information about the employees, from now on they will be informed in connection with contract being signed. This is also evident from the contract. On the established confidentiality agreements, it is evident that the company handles personal information and the obligations that exist. Former employees and consultants will sign a consent.

In addition, the company may be obligated to inform registered persons whose personal information is processed by reason of an assignment. It is important to remember that such information obligation only applies to Data Protection Officers and that there is no information obligation for someone who judges themselves to be a Personal Data Assistant.

The company has drawn up a template to be used to fulfil the information obligation and the handling of employees, clients and contractors. This document will be distributed by e-mail. The client, generally also held as in charge of the personal information given to the company for these purposes (among others, client administration purposes and warranty measures) are in the assignment letter ordered to fulfil the information obligation toward the registered persons regarding the processing that the company will be performing by reason of the assignment.

Article 14 of the GDPR states that there are exceptions form the information obligation. Some of the exceptions mean that the information does not have to be given if the registered person already has the information, if the providing of such information turns out to be impossible or would entail a disproportional effort, if obtaining or disclosure of information is stipulated expressly by law, alternatively if the personal information must remain confidential due to statutory secrecy. In these cases, the Data Protection Officer does not need to inform the registered person about the processing of the registered person's personal information.

To fail to inform registered persons supported by an exception always carries a risk. With reference thereto, and to the transparency principle in place in accordance with the GDPR, the company has drawn up a template for information to the registered persons in the stakeholder register.

To conclude, the company only have a data protection responsibility towards its employees, hired consultants and individuals who have signed up for our stakeholder register. We will handle these in accordance with the new data protection regulation, GDPR.

Personal Data Assistant

The responsibility for setting up a personal data assistant agreement on the one hand rests with the Data Protection Officer (here with reference to warranty issues), but it is in the interest of the personal data assistant to see to it that the role distribution is regulated and that clear instructions be made, since the company in the absence of such not will be able to fulfil its obligations and in addition may be seen as responsible for handling personal information by the regulator for processing of personal information. Some parts of a personal data assistant agreement are obligatory and non-negotiable. If the client wants to use their own template, we must see to it that we do not accept larger responsibility than what is provided in the data protection regulation. Agreements therefore need to be closely reviewed.

The company's own personal data assistants

Regardless of whether we are Data Protection Officers or personal data assistants when it comes to handling personal information within the framework of the operation, we must, when we in our turn hire personal data

assistants, for instance IT services or another sub-contractor, enter into a personal data assistant agreement with such a supplier.

Datainspektionen have come to the conclusion before, that those who hire a cloud service supplier is the Data Protection Officer, wherefore a personal data assistant agreement always must be entered into with the cloud service supplier. To this date, we have entered into personal data assistant agreements with Butik.it and Visma and have thereby fulfilled this requirement.

We process personal information in an adequate way

We have developed routines and ways of working so that personal information is handled in a secure way. The starting point is that only employees within the company who need personal information to perform their duties will have access to them. On the server, only those authorized to use the programs we have on the client are able to use them.

To this date, we have not assessed that we handle especially sensitive personal information and we have therefore not arranged for special authorization checks, who would have a higher protection for personal information. Our security systems are previously developed with a focus on integrity and do to a very high degree protect against intrusion, destruction and other changes that may pose a risk to personal integrity.

We believe that we have good IT security to ensure that personal information is handled securely.

We do not transfer personal information in other cases than expressly described in this policy.

When do we disclose personal information?
Our basis is to never disclose personal information to a third party, unless the person has consented to such disclosure or if it is necessary to fulfil our obligations under law or contract. In the event that we transfer personal information to a third party, there may in special cases be warranted to establish confidentiality agreements, ensuring that personal information is handled in an adequate way. Our template for this purpose must then be used.

Personal data incidents
It is important to know what to do in case there is a personal data incident. A personal data incident or personal data breach is a security incident that for example leads to unintentional or illegal destruction, loss or change of the personal information being processed, consequently are in our register. Also, incidents that lead to unauthorized disclosure or unauthorized access to the personal information being processed, count as personal data breaches. For instance that someone out of curiosity reads or spreads information about certain persons in the company register.

Such an event must according to the main rule be reported to Datainspektionen by the person responsible no later than 72 hours after becoming aware of the personal data breach. The report does not have to be made if there is not even the slightest risk towards the rights of individuals.

Under certain circumstances, the Data Protection Officer may also have to inform the registered persons affected by the incident. What such information must contain and how they should be informed is stated.

Responsibility
MFH/Junior Living are Data Protection Officers, which means that the companies are responsible for how personal information is processed and that the registered persons' rights are protected.

E-mail: info@juniorliving.se
Phone: 08-20 57 50