

# Data protection policy

Contact: Sheila Florell, Compliance Officer, E-mail: sheila.florell@vasakronan.se

This policy describes how Vasakronan processes personal data. All employees at Vasakronan are to process personal data according to the law and this policy.



## General data protection regulation

The General Data Protection Regulation applies from 25 May 2018 in the whole of the EU, and in Sweden complementary national legislation (such as the Data Protection Act and the Camera Surveillance Act) also apply. The General Data Protection Regulation is also known as the GDPR. These regulations aim to protect the individual's privacy regarding how organisations can process personal data.

### Who is responsible for compliance with the regulations?

Final responsibility for personal data lies with the individual who controls processing (the controller). Vasakronan as a company bears the responsibility as controller and shortcomings in processing can lead to high sanction fees and liability to pay damages. Within the organisation, Vasakronan's Chief Information Officer is responsible for compliance with the data protection rules.

### The concepts – personal data and processing

The GDPR applies for **processing personal data**. Personal data is any kind of information that directly or indirectly relates to a living, physical person. Examples of direct personal data are name, personal identification number, telephone number, address, photographs, films, sound recordings, personal preferences and behaviour. Indirect personal data is, for example, apartment number and IP addresses.

As soon as personal data is used, through collection, registration, storage, addition, alteration or use, that constitutes **processing** of personal data. The rules in the GDPR apply to all personal data processing via computer, but in certain cases they can also include manual processing if it is done systematically, for example cataloguing personal data in a filing system. Personal data that is processed in running text, such as on a website or in email, is also covered by the GDPR.

### Sensitive data and criminal data

In the GDPR, special categories of data are defined as **sensitive**, and for these data categories, the basic principle is that processing is prohibited (however, compare with the below, for example regarding employees). Sensitive data is data regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning health or sex life. The prohibition applies not only to data processing that directly reveals or concerns such circumstances, but also if they can be indirectly inferred.

For **criminal data**, the basic principle is that such data regarding breaches of the law is never to be processed. There are, however, certain exceptions. Despite the prohibition, criminal data can be processed if it is necessary to handle a legal claim or fulfil a legal undertaking, for example when a crime



constitutes grounds for termination of an agreement. In this case, the General Counsel at Vasakronan should be notified.

### Purpose and necessary personal data

Personal data may only be collected for pre-determined, specified, explicit and legitimate **purposes**. Personal data may not be processed for any other purpose other than the purpose for which the personal data was collected. The personal data must be correct and relevant in relation to the purpose of the processing. It is not permitted to process more personal data than what is **necessary** with respect to the purpose.

### Legal grounds

A valid legal ground is required for the processing of personal data. Provided that the aforementioned conditions in the preceding paragraph are met, personal data can be processed by private organisations such as Vasakronan according to the following grounds:

1. if it is necessary for entering into or the upholding of a **contract** with the data subject (that is, the natural person whose data is being processed),
2. if the data subject has given **consent** to the processing, or
3. if it is necessary for compliance with a **legal obligation**, or
4. after a **balance of interests**.

### Consent

The legal ground of consent entails that the data subject has agreed to the processing of their personal data after having received clear information. A common misconception is that consent can always be used, or is always required, for the right to process a subject's personal data. But in many cases, it is neither appropriate nor possible to rely on consent. Vasakronan bears responsibility for consent being appropriate and meeting the requirements. To be appropriate, consent must be **freely given** and is not permitted to encompass unnecessary requirements. Furthermore, the data subject must always be able to decline without suffering any consequences. Moreover, the balance of power must be **equal**, which is generally not considered the case, such as between an employer and an employee. In addition, consent must always be possible to **withdraw**, whereupon processing must cease. Accordingly, if we can use any of the other legal grounds for processing personal data, we may not and should not obtain consent.

### Balance of interests

Personal data processing is lawful if it is necessary to satisfy Vasakronan's **legitimate interests** – that is, if these interests override the data subject's interest in protection of their personal data. An assessment of what constitutes legitimate interest must be made for **each individual case**. What must be balanced the context in which the data occurs, what type of personal data it comprises, the purpose for which it is being processed, how it has been disseminated or is at risk of being disseminated as well as what the processing can result in. The content of the data also affects the balance of interests

### Access to personal data

Access to personal data is limited to the employees who need access to current personal data to perform their tasks, for example working with employee issues, contract termination and collection matters or management. If you save documents that contain personal data, access should be limited to those who need it to perform their tasks. Evaluative, harassing or otherwise discriminatory opinions and phrasings may not, under any circumstances, be entered into Vasakronan's data systems. Phrasings such as "slow payer" may therefore not be used – though facts about lapsed payments are to be registered.



## Customers, Suppliers and Stakeholders

### If no contractual relationship exists

The following applies if no contractual relationship applies, regardless of whether one is entered into in the future.

Each time personal data is processed, a **balance of interests** (see above) between Vasakronan's commercial interest in using personal data for sending out invitations and the data subject's interest in protecting their personal data should be conducted. Interest in marketing properties and services is normally one such legitimate interest that gives Vasakronan the right to process personal data, as long as the personal data only consists of names and contact details. Even in the above case, processing must proceed in accordance with the fundamental legal requirements. See more under "Information and deletion of data."

### If a contractual relationship exists

In this case, Vasakronan has the right to process the personal data necessary for performance of the contractual relationship with the data subject as a private person (for example, residential tenants or sole proprietorships) since the **contract** provides the legal ground. Vasakronan may also process the personal data of representatives and contacts for legal entities, with the **balance of interests** comprising the legal ground. This pertains to tenants of premises, suppliers or contractors (that are not sole proprietorships).

Examples of personal data (besides contact and identifying information) that are relevant for a contractual relationship can be lapses in payment and particularly in relation to rental relationships: disturbances, breaches of the tenant's care duties, rules for order and good condition. Processing of personal data is also lawful if it is for exercising legal rights, for example to conduct or complete termination of a contract or to pursue a legal claim. This legal ground may not be used for processing personal data that is not required for the fulfilment of the contract. In this case, a balance of interests must be conducted instead, see above.

### Particular for residential tenants

For the purpose of creating a shared good practice for the processing of personal data in the residential rental market, the Swedish Property Federation and the Swedish Housing Association of Municipal Housing Companies have prepared guidelines. The guidelines have been submitted to the Swedish Authority for Privacy Protection for approval. The guidelines are regarded as good practice within the industry, so they should be followed. The guidelines are available on the Swedish Property Federation's website and on Vasakronan's intranet.

### Particular for Arena

Vasakronan has separate member contracts for the Vasakronan Arena concept. These are primarily signed with companies. Personal data pertaining to representatives and contacts at the member companies are processed on the legal ground of a balance of interests. In the event that the legal ground comprises consent, Vasakronan provides separate information in this regard, for example if you order lunch from us and inform of an allergy. If you use a service in/via Arena that is not provided directly by Vasakronan, we will direct you to the information provided by the respective service provider.

### Marketing and direct marketing

Vasakronan must provide information if personal data will be processed for marketing purposes, regardless of whether a contractual relationship applies. See more under "Information and deletion of data." If personal data is collected and used for marketing or direct marketing purposes, good practice must be followed in this area. If someone contacts Vasakronan to request registration to receive information, a balance of interests can be considered a legal ground for such processing. However, the



data subject must receive information pursuant to the legal requirements. In this case, good practice refers to Swedish Data & Marketing Association's (SWEDMA) rules prepared in collaboration with the Swedish Authority for Privacy Protection and which can be found on SWEDMA's website.

## Information, deletion of data and disclosure

### Information

Vasakronan must inform the data subject of **any type of personal data processing**. Information should be provided as soon as personal data is collected directly from the data subject.

The information to be provided is: Vasakronan's name, address, phone number, corporate registration number and a description of the purpose of the processing. Vasakronan must also state which personal data is to be processed, the legal grounds for the processing, the routines for deletion of data and, if applicable, which data that eventually can be disclosed. The data subject will also be informed of the possibility of altering or erasing their data, as well as how to file a complaint with the Swedish Authority for Privacy Protection if, in the data subject's opinion, their personal data has been processed incorrectly. This information is to be brief, easily comprehensible and expressed in clear, simple language. If personal data is collected from another source other than the data subject, that information is to be supplied upon first contact with the data subject or within a reasonable period of time no longer than one month, and Vasakronan is also to provide information about which source it was.

When a new contact is registered in Vasakronan's register for customers, suppliers and stakeholders, the information will be sent out automatically to the data subject in connection with registration, or otherwise within 30 days if the data is taken from a source other than the data subject. Vasakronan will also provide information about the main principles for the personal data processing that can arise during operations. All employees are to have a link to information about Vasakronan's processing of personal data on the web page in their email signature. You can contact the Legal department, which has templates for information for different situations.

If the data subject **opposes** Vasakronan's processing of their personal data, the basic principle is that this must be noted and the data erased immediately. There are some exceptions to this rule, so you should consult the Legal department in the event of any uncertainty.

### Deletion of data

Personal data may not be saved longer than what is **necessary** with respect to the purpose for which it was collected. When a contractual relationship ends, personal data is deleted after a set period of time. Personal data that does not need to be deleted immediately when the contractual relationship ends includes information in rental agreements or other contracts, which may be saved as long as necessary to monitor remaining claims or as long as required by accounting regulations. In practice, this means that data often may not be saved for longer than seven years.

The rules for deletion of data regarding residential tenants are regulated in the Swedish Property Federation's guidelines (above). Vasakronan's personal data processing list sets out the respective processing/systems' procedures for deleting data.

### Disclosing personal data

Personal data may only be disclosed to third parties if:

- a **contract with** the data subject is to be performed,
- the obligation to disclose the data **is required by law**, or
- the data subject has given **consent**.

If Vasakronan wants to process the data for purposes other than what the data subject can be expected to anticipate, the data subject in question must be informed about the processing, see more below.



## Right to information, alteration, deletion and to withdraw consent

The general information about protection of privacy on Vasakronan's website contains links to pages where individuals can request a copy of the entries in the register, alteration, deletion or data portability. The data subject can also withdraw previously given consent for processing.

## Personal data breaches

A personal data breach arises in any case where Vasakronan loses control over the personal data for which it is responsible. This could comprise a breach of IT systems, but applies equally if you lose your computer, tablet, phone, etc. Moreover, an email containing personal data that has been accidentally sent to an unauthorised person also comprises a breach. If you suspect any leak of personal data you are processing to unauthorised parties, you should immediately report it to IT support.

There is a link on Vasakronan's web page to a form where external parties, for example Vasakronan's personal data processors, can report personal data breaches. This link can be used by employees and external parties if they suspect a personal data breach and the IT department will investigate what has happened.

## Vasakronan's whistle-blower system

Vasakronan has established a whistle-blower system that is managed by an external supplier, Interaktiv Säkerhet AB, through its subsidiary, Whistleblowing Solutions AB, which provides the system. This system acts as a complement to the ability to report improprieties to the General Counsel/Compliance Officer. The objective with this is to provide a safe and secure workplace and to investigate any possibility of the contrary. A whistle-blower service helps individuals report incidents, irregularities and material misconduct. Employees may be included in our whistle-blower service – either as an identified subject of the report or as a witness or a victim. The Swedish Act on the Protection of Persons Reporting Irregularities (2021:890) (the Whistle-blower Act) permits Vasakronan to process all kinds of personal data necessary for a so-called follow-up case. If circumstances so require, information on your work computer and other communication channels may also be collected. The legal ground for the processing of all personal data in the context of a follow-up case is the Whistle-blower Act. Vasakronan will save personal data for the duration an investigation is ongoing and up to two years after an investigation case has been concluded. Vasakronan will not share information other than as required by legal obligations. Vasakronan's partner, Interaktiv Säkerhet AB and thus Whistleblowing Solutions AB, save personal data while a case is being processed as described above in this paragraph but have no actual access to the information.

## Camera surveillance

Camera surveillance is subject to the GDPR and a separate law (below, the Camera Surveillance Act), which complements the rules under the GDPR. The purpose of the Camera Surveillance Act is to meet the need for camera surveillance for legitimate purposes while protecting individuals against infringement of their personal privacy.

The law applies when cameras are used in a manner that constitutes personal surveillance. The surveillance must always meet the GDPR requirements. This means, inter alia, that Vasakronan must be able to demonstrate the legal ground it has for camera surveillance based on a balance of interests that demonstrates that the need for surveillance overrides the right to privacy of those who might be monitored. Camera surveillance requires a clearly defined interest (so-called legitimate interest) of the property owner, such as for the prevention of crime or accidents, disturbances or substantiating legal claims. Arbitrary camera surveillance is thus not permitted. Vasakronan has a separate procedure in place for performing such a needs analysis.

All camera surveillance by Vasakronan is to be documented and the balance of interest justified in a list.

More extensive camera surveillance is considered a form of personal data processing that could lead



to a high risk in terms of the rights and freedoms of individuals and, accordingly, requires an impact assessment to be conducted.

The Swedish Property Federation's guidelines for camera surveillance also contain what is considered good practice for the lettings market, irrespective of whether the lettings pertain to commercial or private tenants. You will find more detailed information on the intranet on the "Camera surveillance" page.

### **Information and deletion of data**

Vasakronan must always provide information when camera surveillance is in operation. This requirement is met through setting up clear signs designed in accordance with the applicable standards. Signs must clearly show that the area is under camera surveillance. Signs must be of an adequate size to ensure they are difficult to miss and must be located so as to be visible prior to entering an area under surveillance. The data subject is thus given the option of whether or not to enter the area under camera surveillance.

The basic principle is that secrecy applies for all recorded material, and that the material may only be used for the purpose for which it was recorded. As few people as possible should have access to the camera material, and those who process the camera material are to protect it with applicable security measures. With regard to cameras connected to a server, none of Vasakronan's employees nor any insourced personnel are permitted access to the camera footage. The material is only available to Vasakronan's camera surveillance partners. Where cameras are not connected to a server, only one designated employee has access to the camera footage in the properties for which said employee is responsible.

No fixed time limits apply to how long material can be saved. Instead, this depends on how long it is necessary given the intended purpose. The guidance from the Swedish Property Federation states that up to two months may be motivated if, for example, the purpose relates to the prevention or detection of crime. When image or audio files may no longer be preserved, they will be deleted.

Camera material may be disclosed to a prosecutor, the police, Swedish Customs, the Swedish Coast Guard or the Swedish Tax Agency if it is necessary for investigating a crime punishable with prison or to prevent or detect such a crime. Sometimes data may also be disclosed to a municipality or a public authority responsible for rescue services if the data is necessary to prevent a threatened accident or to mitigate the effects of an accident that has already occurred. Vasakronan is not permitted to disclose material at the request of, for example, tenants. If, for example, the request is on behalf of and regarding someone who appears on film Vasakronan must consider such request, but even then there are exceptions. In unclear cases, Vasakronan's General Counsel must always be consulted.

### **Electronic entry systems, visitor registration and personnel register**

The GDPR applies to the use of electronic entry systems, for example entry systems to premises. Personal data can be processed within the framework of an electronic entry system provided that the purpose is to replace a system with traditional keys. Under a balance of interest according to the GDPR (see above), Vasakronan can save logs for other purposes. Logging and saving data about entry to shared spaces can be justified by technical maintenance and troubleshooting, or if a property has experienced disturbances, damage or ongoing extensive theft. The purpose behind visitor registration, in addition to safety and security, is to maintain statistics and optimise the use of premises and properties. The legal grounds for visitor registration also comprises a legitimate interest for Vasakronan to process the personal data.

In certain instances, Vasakronan is obliged by law, such as in its capacity as developer, to provide equipment for electronic personnel registers (such as ID06). A personnel register is a list of the individuals working on the construction site and when they have started and finished each work shift. The purpose behind obliging workers to identify themselves and to register their presence on site is to combat undeclared work and other economic crime, and thus to promote healthy competition. The system also simplifies safety efforts at the worksite. In the case of the personnel register, the legal



ground comprises the fulfilment of legal obligations. If you receive enquiries requesting information from the personnel register, please contact Legal department.

To prevent undue infringements of personal privacy, the number of individuals who have access to the log should be limited, with clear procedures for how the log may be used. A log may, like other registered personal data, not be used in a manner that can entail a risk of infringement of personal privacy. Saving personal data to control individuals in connection with, for example garage entry, shared entrances or to property, can be considered a major infringement of personal privacy. More extensive use of entry systems is considered a form of personal data processing that could lead to a high risk in terms of the rights and freedoms of individuals and, accordingly, requires an impact assessment to be conducted.

Personal data in an entry system will not be stored for longer than necessary for the purpose. To date, the Swedish Authority for Privacy Protection has not encountered any situation where the purpose would justify saving entry logs for longer than two weeks. Accordingly, Vasakronan's entry and visitor systems follow the basic principle and are **deleted after a maximum of two weeks**.

## Employees and contractors

Vasakronan may process personal data if it is necessary for fulfilling the contract of employment, another agreement or due to legal obligations incumbent on Vasakronan from its duty as employer. Employees and contractors have access to separate information with regard to processing personal data.

## List of registers and systems

The registers and systems containing personal data at Vasakronan are summarised in a list of processing activities. It is incumbent on everyone responsible for a register or similar where personal data appears to ensure that the record is updated and its instructions followed.