General information for The Swedish Internet Foundation’s registrars regarding disclosure of personal data

Agent - 2022-06-20 - Legal

This text has been produced by The Swedish Internet Foundation as a general description of the requirements imposed by the General Data Protection Regulation (GDPR) for the disclosure of personal data. Since the responsibility lies with the data controller to make the assessment, a special assessment must be made in each case, and if in doubt, we advise you to contact a legal representative.

Background

As a registrar, it occurs that different actors (for example, official agencies and private individuals) request information related to a domain name.

The registrar’s operations are governed by different rules. Particularly relevant to the registrar’s operations is the GDPR, which regulates how personal data should be processed.

Personal data includes names, personal identity numbers and email addresses. However, any information relating to an identified or identifiable natural person is considered to be personal data. If, e.g., a domain name consists of a first name and surname, the domain name itself can also be personal data since it can be used to identify a natural person.

The GDPR is applicable when personal data is processed fully or partially automatically and applies to other processing of personal data which form part of a filing system or are intended to form part of a filing system. Processing of personal data is any action taken related to personal data. This means that the term processing in the GDPR includes collection, storage and disclosure of personal data.

When the registrar processes personal data in its operations, the registrar is responsible for ensuring that the processing of personal data takes place in accordance with GDPR. In order for the registrar to be compliant with the GDPR, certain considerations must be made before personal data can be disclosed.

Legal basis for disclosing personal data

Background

One basic requirement of the GDPR is that there must be a legal basis to be able to process (e.g., to collect or disclose) personal data. The legal basis includes consent being obtained from the relevant person, there being a legal obligation to process the personal data or a legitimate interest in processing the personal data. The grounds for a legal basis for processing are found in Article 6 of the GDPR.

Consent can be used as a basis to disclose personal data, however, since obtaining consent may be challenging, a consent can be withdrawn and there is a real risk that a consent is not considered valid, consent as a basis for disclosing personal data should be used primarily as a last resort or together with another legal basis. (Consent is a clear affirmative action that involves the freely given, unambigous indication of the data subject's agreement.)

The legal bases that are best suited for the disclosure of personal data are therefore a legal obligation and a legitimate interest. While a legal obligation means that the registrar must disclose certain personal data, a legitimate interest means that the registrar is permitted to disclose the personal data that is necessary to achieve the purpose.

Legal obligation

There are laws, rules and official government decisions alongside the GDPR stating that a registrar must disclose personal data to the party requesting it. For example, a law stating that a supplier is required to provide personal data to an authority or court.

A legal obligation to disclose personal data is primarily relevant if the party requesting the information represents an authority. If a company or individual has gone to a court of law and the court has decided that the registrar is required to disclose certain personal data, it may also be a case of a legal obligation.

An example of a legal obligation to disclose personal data is stated in the Swedish Marketing Act (marknadsföringslagen (2008:486)). Section 42 of the Marketing Act, states that upon request of the Swedish Consumer Ombudsman, everyone must provide the information needed in a matter concerning the application of the Marketing Act. If the Swedish Consumer Ombudsman therefore request some personal data pursuant to Section 42 of the Marketing Act, the registrar must disclose the data that is requested. Similar provisions are included in other legislation, where the rules are usually designed so that a particular authority is given special powers to contact a supplier to access data or information in a matter related to an investigation.

Although many authorities may refer to a provision involving a legal obligation for the registrar to disclose personal data, it is good idea to check and review the rule that the authority provides. If no law or regulation is mentioned and the authority is requesting personal data, the registrar can ask the authority whether there is a legal obligation for the authority’s request. This helps the registrar, who is responsible for the processing of data and for showing compliance with the GDPR.

Legitimate interest

A registrar is also allowed to disclose personal data if there is a legitimate interest, provided that the legitimate interest outweighs the interests and the fundamental freedoms and rights of the person whose personal data is processed. Which interest have priority shall be settled by a balancing of interests. If the registrar, after balancing the interests, finds that the party requesting the data has an interest outweighing that of the person whose

personal data is processed, the personal data necessary to achieve the purpose may be disclosed.

Conducting a balance of interest to examine which personal data may be disclosed may be considered regardless of whether it is an authority, a natural person or a company requesting the personal data. It is important that a concrete balance of interests be carried out in each case.

In order to use the grounds of legitimate interest as basis for disclosing personal data, the registrar needs to know the purpose of the party requesting the personal data and what the personal data is to be used for. Such a legitimate interest can be to prevent fraud or investigate violations. A legitimate interest may also exist if the party requesting the data wants to get in touch with the domain holder, in order to take over the domain name or to initiate a dispute on a superior right to the domain name, but an assessment needs to be made by the registrar in each individual case. In practice, the balancing of interests must entail the interest of the party requesting the personal data being responsibly weighed against the interest and the rights of the person whose personal data is requested. If the registrar concludes that the interest of the party requesting the data takes precedence, the data may be disclosed.

It is important that the registrar only discloses the personal data that is needed for the party requesting the data to realise the purpose. For example, if a natural person requests information about a domain holder's name, telephone number, e-mail address and personal identity number in order to get in touch with the domain holder, it is probably sufficient that the registrar only disclose the e-mail address of the domain holder in order for the purpose to be achieved.

When personal data has been disclosed after a balance of interests, it is important that the registrar document the assessment, to be able to show that GDPR is complied with. This documentation can be requested by the data protection authority.

Final considerations

The GDPR sets certain requirements on how the registrar is to manage personal data in its operations.

As the data protection authorities exercise supervision over the application of the GDPR, additional information will be provided on both the grounds of legal obligation and legitimate interest to disclose personal data. New guidelines on the GDPR are published continuously on The Swedish Data Protection Authority's website.

Until then, a large part of working with GDPR is about thinking before taking measures that concern personal data and always having to consider that personal data should be processed in a protective manner.