

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision 2022-01-19, no. DI-2021-4741. Only the Swedish version of the decision is deemed authentic.

Our ref.:
DI-2021-4741

Date of decision:
2021-12-19

Date of translation:
2022-01-20

Supervision under the General Data Protection Regulation – One.com Group AB

Final decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy protection finds that One.com Group AB has processed personal data in violation of Article 6(1)(f) of the GDPR¹ by processing data about the complainant's first name and surname, address, telephone number in confirmation e-mails, without it being necessary, for the legitimate interest of ensuring the identity of the person who changes contact details for a registered domain.

The Swedish Authority for Privacy Protection gives One.com Group AB a reprimand in accordance with Article 58(2)(b) of the GDPR.

Description of the supervisory case

The case handling

The Swedish Authority for Privacy Protection (IMY) has initiated supervision of One.com Group AB (One.com or the company) due to a complaint. The complaint has been submitted to IMY, in its capacity as responsible supervisory authority pursuant to Article 56 of the GDPR. The handover has been made from the supervisory authority of the country where the complainant has lodged the complaint (Germany) in accordance with the Regulation's provisions on cooperation concerning cross-border processing.

The investigation at IMY has been carried out in written form. In the light of cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The supervisory authorities concerned have been the data protection authorities in Germany, Poland, Norway, Ireland, Denmark, France and Italy.

The complaint

The complaint has, in essence, stated the following. The complainant wished to change the contact details (e-mail address) of a registered domain at One.com. The

Postal address:
Box 8114
104 20 Stockholm
Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
+46 (8) 657 61 00

¹ Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with respect to the processing of personal data and on the free flow of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

complainant contacted the company and informed that the previously registered e-mail address would need to be changed due to inactivity. The complainant was then asked to complete a form and attach a copy of their identity document. The e-mail address previously provided by the complainant had, at that time, been inactive for approximately three years. After the change of contact information (e-mail address) the company sent out a confirmation e-mail about the change to both the previous and the new e-mail address. The confirmation e-mail contained the complainant's personal data. Since the complainant has not been using the previously provided e-mail address for several years, they consider that the verification mailing to the previously given address is a violation of the GDPR. The complainant further states that they have not given consent to the processing and that the data may have been disclosed to unauthorized persons.

What One.com has stated

One.com has, in essence, stated the following.

One.com is the controller of the personal data concerned in the complaint.

It is correct that a confirmation e-mail is sent out when a domain owner wishes to change contact details (e-mail address). The e-mail contains the complainant's first name and surname, address, telephone number and e-mail address.

The company states that the lawful basis for sending personal data to both the previous and the new e-mail address is Article 6(1)(f) (legitimate interests). The purpose of the processing is to ensure the identity of the account holder, that changes to contact details (e-mail address) are done at the initiative of the account owner and to ensure that the holder of the new e-mail address receives information and accepts that it is linked to an account at One.com (this should be the same person). The company states that the procedure also ensures that the company fulfils its contractual obligations towards the account holder. Thus, according to the company, there is also a commercially justified purpose.

When an account is created on One.com, one of the main elements is the e-mail address to which the account is linked. The company informs anyone who creates a new account that the account is linked to the e-mail address provided by the account creator. The company, therefore, considers itself transparent with its personal data processing.

As the mailings only contain necessary, general personal data, the company states that the rights and freedoms of the data subjects do not override the legitimate purposes of the company.

As an account is linked to the e-mail address initially provided by the account creator, the company uses a copy of the account holder's identity document together with e-mail verification as a two-factor authentication. It is done to ensure that the change of contact details (e-mail address) is approved by the account holder and to ensure that the company complies with its obligations towards the account holder under the agreement. Only a copy of an identity document could not fulfil the same purpose.

Summary of the company's statements

The purpose of the data processing

The company states that they have an interest in processing personal data in the e-mail verification for the following purposes:

- to ensure the identity of the account holder;
- to ensure that the change of contact details takes place at the initiative of the account owner;
- to ensure that the account holder of the new e-mail address accepts that the address is linked to an account at One.com; and
- to ensure that the company complies with its contractual obligations towards the account holder.

The necessity of the data processing

The company states that the processing of personal data in the e-mail verification is necessary because:

- the e-mail verification is part of a two-factor authentication of the account holder;
- only a copy of the identification document does not fulfil the purpose of verification; and
- the company needs to verify that the change to the contact information has been initiated by the account holder.

Balancing of the legitimate purpose of the company and the rights and freedoms of the data subjects

The nature of the personal data

The email contains the complainant's first name and surname, address, telephone number and e-mail address, which does not constitute sensitive personal data.

Reasonable expectations

The company considers that the personal data processing in question is transparent in relation to account holders because the company informs those who open an account with One.com that the account is linked to the email address chosen.

The company's view is that the fundamental rights and freedoms of the data subjects do not therefore override the interests of the company.

Justification of decisions

Applicable provisions

In order for a personal data processing to be considered lawful, it is necessary that at least one of the conditions set out in Article 6(1) GDPR is fulfilled.

For processing to be able to rely on Article 6(1)(f), three conditions needs to be filled: (1) the controller or third party has a legitimate interest (legitimate interest), (2) the processing is necessary for the purposes of the legitimate interest (necessary) and (3) that the interests or fundamental rights and freedoms of the data subject do not override and require the protection of personal data (balance of interests).

It follows from the case-law of the Court of Justice of the European Union that exceptions and limitations to the protection of personal data must be limited to what is strictly necessary.² Furthermore, the condition required by Article 6(1)(f) must be examined in conjunction with the principle of data minimisation (Article 5(1)(c)). This presupposes that the legitimate interest which the processing is intended to protect cannot reasonably be protected as effectively by other means which less adversely affect the fundamental rights and freedoms of data subjects, and that no more data than is necessary is processed.³

Recital 47 states that the legitimate interests of a controller may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing

Assessment of the Swedish Authority for Privacy Protection

IMY considers that the interests presented by the company are justified, having regard in particular the fact that the processing of personal data contained in the e-mail verification:

- is part of a two-factor verification;
- ensures that the change of contact details has been initiated by the account holder; and
- ensures that the holder of the new registered e-mail address accepts that the address is linked to an account at One.com.

IMY has now to consider whether all the personal data contained in the confirmation e-mails were necessary in relation to the purpose. IMY does not dispute that the company sent confirmation e-mails to the complainant's previously registered and new e-mail address based on the legitimate interest. However, IMY considers that the purpose of the confirmation e-mails, to ensure that the contact details are changed by the right person, can be achieved without mentioning the complainant's first name, surname, address and telephone number. Given that all the personal data contained in the confirmation e-mail were not necessary to protect the legitimate interest, the processing is not lawful on the basis of legitimate interests.

IMY therefore finds that One.com has violated Article 6(1)(f) of the GDPR by processing personal data in a confirmation e-mail without it being necessary in relation to the purpose of the processing.

² Case C-13/16 Rīgas satiksme', Judgement of 4 May 2017, para. 30.

³ Case C-708/18 TK v Asociația de Proprietari bloc M5A-ScaraA, Judgement of 11 December 2019, paras. 46-51. The Court of Justice has also confirmed that that case-law continues to apply in the context of the GDPR; Case C-597/19 M.I.C.M., Judgement of 17 June 2021, para. 107.

Choice of corrective measure

Pursuant to Article 58(2)(i) and Article 83(2) IMY has the authority to impose administrative fines in accordance with Article 83. Depending on the circumstances of the individual case, administrative fines may be imposed in addition to or instead of the other measures referred to in Article 58(2). Furthermore, Article 83(2) states which factors should be taken into account in decisions on whether administrative fines should be imposed and when determining the amount of the fine. In case of a minor infringement, IMY may, as stated in Recital 148, instead of imposing a sanction fee, issue a reprimand pursuant to Article 58(2)(b). In this assessment, regard shall be taken to aggravating and mitigating circumstances in the case, such as the nature of the infringement, severity and duration as well as previous infringement of relevance.

IMY notes the following relevant facts. The violation has affected one person and it has not concerned sensitive data. IMY has not previously established that the company has infringed the GDPR. Furthermore, the investigation has not shown that there has been any disclosure of personal data to a third party. One.com clearly informs its customers that they have an obligation to keep their contact details up to date.⁴ At the time of the change, the applicant's previous e-mail address had been inactive for about three years. In an overall assessment of the circumstances and the nature of the infringement, IMY considers that it is a matter of a minor infringement within the meaning of recital 148 and that One.com should be given a reprimand pursuant to Article 58(2)(b) of the GDPR for the stated infringement.

The case is closed.

This decision has been made by the specially appointed decision-maker [REDACTED]
[REDACTED] after presentation by legal advisor [REDACTED]

⁴ <https://www.one.com/en/terms-and-conditions-usd>

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact information is shown in the first page of the decision.