Swedish Authority for Privacy Protection

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) final decision 2022-10-10, no. DI-2021-3399. Only the Swedish version of the decision is deemed authentic.

Ref no:
DI-2021-3399, IMI case no. 115749

Date of final decision:
2022-10-10

Date of translation:
2022-10-11

Final decision under the General Data Protection Regulation – Trionic Sverige AB

Decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection (IMY) finds that Trionic Sverige AB has processed personal data in breach of

- Article 6(1) of the General Data Protection Regulation (GDPR)[1] by disclosing the complainant's personal data with a third party without it being necessary to comply with a legal obligation,
- Article 13(1)(e) by providing the complainant with insufficiently specific information about recipients or categories of recipients of the personal data when processing data for the purpose of combating fraud.

The Swedish Authority for Privacy Protection issues Trionic Sverige AB a reprimand pursuant to Article 58(2)(b) of the GDPR for the infringement of Articles 6(1) and 13(1)(e) of the GDPR.

Presentation of the supervisory case

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

The investigation in the case has been carried out through correspondence. In the light of a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory authorities concerned have been the data protection authorities in Denmark, Norway and Germany.

[1] Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to he processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

The complaint
The complaint states the following.

On behalf of the complainant, a product was ordered via Trionic's German website. According to the complainant Trionic, for some reason became suspicious of the e-mail address used for the order and therefore sent a copy of the order confirmation to the info-e-mail address provided in the domain where the complainant has their e-mail address.

Trionic also sent information about the order to a company even though it was not apparent from the privacy policy that data will be shared with that company. Furthermore, as of 1 July 2018, the privacy policy is not easily accessible. Clicking on the "Privacy Policy" link on Trionic's website opens a new page on the website that links further to the policy located on another website.

Trionic also reportedly Google searched the name, address and contact details of the complainant's representative and possibly linked that information to the complainant's data. Trionic has also stored the entire IPv6 number used when ordering. The privacy policy states that IP numbers are only processed for operation and maintenance purposes. Trionic has also continued to store the IP number even after the complainant canceled the order.

What Trionic Sverige AB has stated
Trionic has mainly stated the following. The company is the data controller for the processing to which the complaint relates.

Transfer to info-e-mail address on the basis of a legal obligation
Trionic sent a copy of the complainant's order to an info-e-mail address on the basis of a legal obligation. Trionic is obliged to take all reasonable steps to ensure that personal data that are inaccurate in relation to the purposes for which they are processed are deleted or rectified without delay (cf. Art. 5(1)(d) GDPR). Trionic's main target group is people in the age range 60-90 years. It is common for the company's customers to make unintentional errors when ordering form in the company's online store.

When the company checked the details of the complainant's order, it reacted to the fact that the e-mail address contained Trionic's company name and the company therefore believed that the buyer had provided an invalid e-mail address. The company then attempted to contact the customer through the given telephone number in order to correct the e-mail address provided. The phone number turned out to be a fax number. In the absence of other contact details, the company visited the domain name of the email address. There the company found the info-e-mail address that the company, for valid reasons, thought was the correct e-mail address. The company then replaced the customer's e-mail address with the one found and sent the order confirmation to that e-mail address. At the time, the company considered that it was its' only possibility to correct the customer's contact details and that the measure therefore was necessary.

When Trionic became aware of the mistake, the company found that it was unlikely that it had resulted in any risk to the complainant's personal integrity. The reason for this was, in particular, that the circumstances indicated that the complainant's personal data had been disclosed to a very limited circle of (other than the complainant) a family member and that it was personal data of relatively limited integrity value.

Legal basis for disclosure to combat fraud

Trionic has disclosed personal data relating to the complainant to a provider of fraud control services on the basis of a legitimate interest which, at the time, acted as a data processor to the company.

The information disclosed consisted of the complainant's name, e-mail address, information that it is the complainant's first purchase from Trionic, the complainant's e-mail domain name, telephone number, order number, number of items purchased, currency of the purchase, the value of the purchase, the complainant's invoice, delivery and IP address.

On the German market, Trionic offers its customers to pay by invoice. It is Trionic that issues the invoice and accounts for the credit risk. Over the years, Trionic has been subject to a number of frauds and fraud attempts in the form of customers who choose to purchase products with invoice payment without the intention to actually pay the invoice. In order to prevent fraud (the purpose of the processing), Trionic has therefore used the services of the provider. The data in question have been disclosed to the service provider on the basis of Trionic's legitimate interest to prevent fraud. Following a balancing test considering the complainant's interests and fundamental rights and freedoms as set out below, Trionic considers that it has had a legal basis for the processing.

The processing was *necessary* to achieve the purpose on the following grounds. The complainant chose to pay by invoice. The data provided by the customer differed from the norm, in that the fax number had been entered instead of a regular telephone number and the e-mail address contained the word "Trionic". Trionic is responsible for the credit risk of invoice purchases on the German market and fraud attempts are common for credit purchases in e-commerce.[2] About two percent of all purchases in Trionic's online store have been flagged as suspicious by the supplier. Furthermore, Trionic lacks the competence and resources to perform the type of analysis offered by the supplier. Against this background, there were no alternatives to the processing in order to achieve the objective of fraud prevention.

As regards to what the data subject *can reasonably expect*, the company notes that the type of analysis offered by the supplier in the context of credit purchases is common in e-commerce on the European market. The aim is to prevent fraud. It constitutes a type of supplement to credit assessment. A credit assessment can show that a buyer is creditworthy, but not that the buyer is indeed the person to whom the credit assessment relates and that the buyer has a real intention to pay for the purchase. Therefore, in the case of online credit purchases, consumers must expect this type of assessment to be carried out.

Regarding the *nature of the data*, Trionic argues that the supplier's analysis was based entirely on the above-mentioned personal data that Trionic shared with the supplier. This data typically has a relatively limited integrity value, as in many cases it is publicly available.

As regards the *negative consequences*, according to Trionic, the potentially negative consequence of the processing for the complainant is that the credit purchase would be refused, which is a relatively mild consequence that should not affect the outcome of the balancing of interests.

[2] See for example: https://www.svenskhandel.se/sakerhetscenter/amnesomraden/bedragerier/

Legal basis for the processing and storage of IP address prior to cancellation
The complainant's IP address was stored and transferred to the supplier for the purpose of analysing the complainant's geographical location at the time of ordering. These processing operations were carried out for the purposes of fraud prevention (Objective 1) and for the purpose of identifying and asserting legal interests (Objective 2).

The purpose of fraud prevention is a legitimate interest of Trionic. With regard to the necessity of the processing, it can be noted that in the case of fraud attempts, the place of purchase and delivery often does not match the location of the IP address and the customer's connection. Along with other warning signs, such as incorrect phone numbers and a possible IP address connected via anonymisation services, it helps Trionic avoid fraud. Often, fraudulent buyers have several different e-mail addresses but usually do not exchange IP address. Therefore, by saving and processing buyers' IP addresses, Trionic can check the total amount of orders made in the web shop with the same IP address. Without saving the IP address, none of this would have been possible.

With regard to what the data subject *reasonably can expect*, reference is made to the corresponding assessment regarding the disclosure of anti-fraud data as set out above.

As for the *purpose of establishing and exercising legal claims*, Trionic has a legitimate interest in storing the IP address used in purchases in order to establish and enforce legal claims, both civil (debt collection) and criminal law (as a plaintiff in fraud investigations). As regards the necessity of processing, in the case of online credit purchases without the use of e-identification, there is no better opportunity to establish the actual identity of the buyer than to document the IP address used in the purchase. Proof of the identity of the buyer is directly necessary in order to recover past due claims and to obtain conviction in the event of fraud.

Regarding what *the data subject can reasonably expect*, Trionic has made the assessment that from the point of view of the data subject it should appear more or less obvious that e-commerce companies save the IP address of the credit purchaser in connection with purchases in order to be able, if necessary, to establish the identity of the buyer and to recover past due claims and to be able to pursue criminal claims in the event of fraud. Furthermore, Trionic has considered that the IP address has a limited privacy value that does not outweigh Trionic's need to establish and enforce legal claims and that the processing does not risk to cause any significant consequences for buyers. The most obvious consequence may be that the purchase will be denied.

Legal basis for continued storage of IP address after cancellation
Trionic continued to save the complainant's IP address for the purchase after the order was cancelled. However, Trionic deleted it after receiving the complaint, which it interpreted as a request for deletion.

Trionic considers that the company has a legitimate interest in saving the IP address used for the purchase in order to establish and enforce legal claims, both civil (receivable recovery) and criminal law (as plaintiff in fraud investigations). This also applies in the case of cancellations as it may have civil and criminal implications within the limitation period.

The processing is necessary in the same way as before cancellation.

Concerning what the data subject could reasonably expect, it is the same as for storage prior to cancellation, with the addition that, in Trionic's view, the assessment is not affected by the fact that it concerns a cancelled purchase, since it may have civil and criminal implications within the limitation period. However, as mentioned above, after receiving the complaint, Trionic decided to delete the complainant's IP address.

Easily accessible information to the data subject
Trionic states that before confirming the purchase, the complainant had the opportunity to read Trionic's Privacy Policy by clicking on a link in the text "[I] have read the Terms and Conditions and Privacy Policy and approves them." It was then also possible for the complainant to access the Privacy Policy by clicking on a link on the company's website. Due to a loading error, at the time of the complaint, two clicks were required to reach the privacy policy, which has since been corrected. The policy could also be accessed by just one click on a link to the policy at the bottom of the footer of the Trionic website.

Information on the processing to combat fraud and the storage of IP addresses
As regards information on anti-fraud, the processing activities section states:

"Data processing is carried out using computers or IT-based systems in accordance with organisational procedures, which are specifically aimed at the stated purposes. In addition to the responsible person, other internal personnel (personnel management, sales, marketing, legal department, system administrators), or external resource — with the responsible person as principal (such as technical service providers, delivery companies, hosting providers, IT companies or communication agencies) — may operate this website and thus have access to the information. An up-to-date list of these participants may be requested at any time from the provider (Trionic)."[3]

Trionic is aware of its obligation under Article 13 of the GDPR to inform about the recipients or categories of recipients who are to access the personal data. The text above states, inter alia, that Trionic may pass on personal data to external resources. With the complainant's complaint, the company has reviewed the privacy policy and decided to amend it to explicitly indicate that personal data may be disclosed to companies that analyse the fraud risk of credit purchases.

With regard to information about the *storage of the IP address*, the Privacy Policy specifies which data is processed by Trionic or by third parties. It states that so-called "user data" is stored when it is provided voluntarily by the user or collected automatically when using the online store and includes the user's IP address. Furthermore, it is clear that collected personal data may be processed in order to safeguard Trionic's rights and interests. Trionic informed about this in the same way as in the case of anti-fraud.

[3] Unofficial translation made by the Swedish Authority for Privacy Protection. Original wording: *Databehandlingen utförs med hjälp av datorer eller IT-baserade system enligt organisatoriska förfaranden, som är specifikt inriktade på de angivna syftena. Förutom den ansvariga personen kan annan intern personal (personalhantering, försäljning, marknadsföring, juridisk avdelning, systemadministratörer), eller extern resurs - med den ansvariga person som uppdragsgivare (såsom leverantörer av tekniska tjänster, leveransföretag, värdleverantörer, IT-företag eller kommunikationsbyråer) - driva denna webbplats och därmed ha tillgång till informationen. En aktuell lista över dessa deltagare kan när som helst begäras från leverantören (Trionic).*

Search for the applicant's data via search engines
Trionic has not sought the stated contact details on Google and brought them together with the complainant's data as alleged in the complaint.

Justification of the decision

Applicable provisions, etc.

Article 6(1) of the GDPR contains a list of possible legal bases for processing of personal data. One of the legal bases set out in this paragraph must be applicable in order for the processing to be lawful. The points applicable in the case are points 6(1)(c) and (f).

According to Article 6(1)(c), processing is lawful if it is necessary for the performance of a legal obligation incumbent the controller.

In order for processing to be based on Article 6(1)(f), all three conditions provided therein must be fulfilled, namely, firstly, that the controller or third party has a legitimate interest (*legitimate interest*), secondly that the processing is necessary for purposes of legitimate interest (*necessary*) and third that the interests or fundamental rights and freedoms of the data subject do not weigh heavier and require the protection of personal data (*balance of interest*).

Recital 47 of the GDPR states that processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. Furthermore, the Article 29 Working Party[4] has previously stated that preventing abuse is a legitimate interest under the corresponding rules of the previously applicable Data Protection Directive, as long as the interest is "acceptable under the law" in the broadest sense of the term.[5]

Article 13 sets out the information to be provided by the controller to the data subject where the personal data are collected from the data subject. Under Article 13(1)(e) the controller shall provide the data subject with information on the recipients or categories of recipients of the personal data. According to Article 4(9), the term "recipient" means for an example a natural or legal person to whom the personal data are disclosed, whether a third party or not.

Assessment of the Authority for Privacy Protection (IMY)

Legal basis
Transfer to the info e-mail address on the basis of a legal obligation
Trionic stats that the sending of the complainant's order confirmation to the info-e-mail address — which was a different e-mail address from the one that the complainant filled in — was made on the basis of a legal obligation. The obligation is to comply with the obligation under Article 5(1)(d) GDPR to take all reasonable steps to ensure that personal data that are inaccurate in relation to the purposes for which they are processed are deleted or rectified without delay.

[4] The Working Party was established under Article 29 of Directive 95/46/EC and was an independent EU advisory body on data protection and privacy issues. With the entry into force of the GDPR, he Working Party has been replaced by the European Data Protection Board (EDPB) (see Articles 68 and 94(2) of the GDPR).
[5] Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC of 9 April 2014, WP 217, p. 25.

IMY notes that although Article 5(1)(d) constitutes a legal obligation for Trionic, it only permits the processing of personal data that is necessary. IMY observes that there were less coercive measures which the company could have taken that would have led to a lower risk of unauthorised disclosure of the complainant's data. For example, Trionic could have sent the order to the stated e-mail address and consider further measures, for example, if the company received an automatic e-mail server response that the message could not be delivered. The company could also have, for example, refrained from processing the order until the complainant contacted them again, send a regular letter to the address filled in by the complainant or send a fax to the fax number indicated. IMY therefore concludes that the processing was not necessary and that the company did not demonstrated that the processing could be based on this legal basis.

Since it has not been established that Trionic had any other legal basis for the processing, the company has therefor processed the complainant’s personal data in breach of Article 6(1) and thus not met the requirement to have a legal basis for the processing.

Legal basis for disclosure to combat fraud

The investigation shows that Trionic has disclosed the complainant's personal data to a provider offering anti-fraud services. Trionic argues that the processing had a legal basis in the company’s legitimate interest in preventing fraud, i.e. Article 6(1)(f) of the GDPR.

IMY notes that it is therefore necessary for the company to be able to demonstrate that three conditions are met:

- there are one or more *legitimate interests*
- the processing of personal data is *necessary* for a purpose relating to the legitimate interests
- the interests or fundamental rights and freedoms of data subjects *do not outweigh* the company’s legitimate interests (balance of interests).

IMY notes that what may be a *legitimate interest* should be interpreted broadly. The decisive factor is whether the interest is permitted by law or otherwise generally recognised in the rule of law. Insignificant interests do not weigh as heavily as important or compelling interests, but are important only in the balancing of interests. However, if an interest is not justified and legitimate, the balancing of interests shall not be carried out, as the initial threshold of this legal basis will not be reached.

It must also be an *actual interest* at the time of the processing and not an interest which is hypothetical at that time. If there are evidence that the interest is not hypothetical, the condition is satisfied, but it may also be sufficient that the interest typically appears to be factual.

IMY finds that the interest presented by Trionic — to prevent fraud — was justified (cf. recital 47 of the GDPR) and actual at the time of processing.

IMY notes that the requirement of *necessity* means that the interests which the processing is intended to protect could not reasonably be protected in an equally effective manner by other means less intrusive on the fundamental rights and freedoms of data subjects. The condition must be examined together with the principle

of data minimisation which means, among other things, that personal data should not be processed unnecessarily.

According to IMY, the processing — the disclosure of the data to the anti-fraud service provider — was necessary in order to fulfil the purpose which Trionic could not reasonably fulfil in an equally effective manner by, for example, carrying out such an assessment itself. This assessment also considers the fact that the disclosure was not too extensive or privacy sensitive in itself.

IMY notes that the third condition under Article 6(1)(f), *balancing of interests*, is carried out by making an overall assessment, considering in particular:

- the seriousness of the violation that the processing entails for the data subject
- what data subjects reasonably can expect in that situation and
- what security measures have been taken.

When balancing the company's legitimate interests on one hand against the complainant's interests, rights and freedoms on the other, IMY finds that the company's interests weighs heavily especially considering it is a credit purchase. This must be weighed against the complainant's interest in not having their data processed or not risking being denied the purchase of the credit.

The processing appears, in IMY's view, to be something that the complainant could reasonably expect when making a credit purchase on invoice, despite the minor deficiencies in the information identified below by IMY in relation to the information provided on that category of recipients of the data. With regard to the seriousness of the violation, IMY finds that the processing does not appear to be highly violating of privacy and that the data itself is not privacy sensitive. When it comes to protective measures, there has been no evidence of relevance for the assessment in this case.

In an overall assessment IMY finds that the company has shown that the complainant's interests or fundamental rights and freedoms do not outweigh the company's legitimate interests for the processing.

In conclusion, the company has demonstrated that the conditions laid down in Article 6(1)(f) are met and the company therefore had a legal basis for the processing.

Legal basis for the processing and storage of IP address prior to cancellation
Trionic states that it processed and stored the complainant's IP address prior to cancellation on the basis of the legitimate interests of (1) preventing fraud and (2) being able to establish and enforce legal interests.

IMY has already considered that the disclosure of, inter alia, the complainant's IP number in order to prevent fraud had a legal basis. There has been no reason to make any other assessment regarding Trionic's own continued processing and storage of that information before the complainant cancelled their order.

Furthermore, IMY considers that there were no grounds for calling into question the legality of Trionic's processing before the cancellation was made in order for Trionic to be able to establish and enforce legal claims.

The processing of the complainant's IP number therefore had a legal basis.

Legal basis for processing and storing IP address after cancellation
Trionic states that the complainant's IP address was also saved for a certain period after the order was cancelled, on the basis of its legitimate interest of being able to establish and enforce legal claims. However, the data was deleted after the complainant's request.

In view of the fact that Trionic deleted the data in response to the complainant's request and thereby satisfied the complainant's rights, IMY considers that the subject matter of the complaint has been examined to the extent appropriate. IMY does not therefore investigate whether Trionics had a legal basis for storing the complainant's IP number after the cancellation or whether the company's general storage periods are well balanced.

Easily accessible information to the data subject
It is apparent from the company's own information that, at the time of the complaint, two clicks were required for the complainant (considering the links the complainant chose to fallow) to be able to access Trionic's privacy policy on its website. The investigation also shows that the information was accessible on the website with fewer clicks (one) in two other ways.

Against this background, and the fact that Trionic also has taken steps to ensure that the policy requires only one click, IMY considers that the subject matter of the complaint in this part has been investigated to the extent appropriate.

Information to the data subject on the processing for the purposes of combating fraud and storage of IP address
The investigation shows that Trionic has disclosed the complainant's data to a supplier for the purpose of combating fraud. In order to comply with the obligation to provide information to the complainant, Trionic had indicated in its privacy policy at the time that personal data could be passed on to 'external resources'. Trionic has now changed this information so that it is explicitly stated that personal data may be disclosed to companies that analyse the fraud risk of credit purchases.

IMY considers that the information provided to the complainant — "external resources" — was not sufficiently specific to meet the requirement of Article 13(1)(e) GDPR to inform the data subject about the recipient (the actual provider) or the categories of recipients (anti-fraud service providers) who would receive the personal data in the case. Trionic therefore infringed Article 13(1)(e).

Searching for the complainant's data on search engines
The complainant has stated that Trionic has searched contact details on a search engine and gathered them together with the complainant's data. The statement was rejected as by Trionic.

IMY considers that there has been no reason to question the company's statement. The investigation in the case does not therefore show that Trionic has processed the complainant's personal data in breach of the General Data Protection Regulation in this part.

Choice of corrective measure

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that the IMY has the power to impose administrative fines in accordance with Article 83. Depending on the

circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) provides which factors are to be taken into account when deciding on administrative fines and in determining the amount of the fine. In the case of a minor infringement, as stated in recital 148, IMY may, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Factors to consider are the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and past relevant infringements.

IMY notes the following relevant facts. The violations have affected one person, the personal data in question was not privacy-sensitive and the company has not previously been found to have infringed the GDPR. Furthermore, Trionic Sverige AB has improved its information to data subjects and acted in response to the complaint.

Against this background IMY considers that it is a minor infringement within the meaning of recital 148 and that Trionic Sverige AB must be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

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

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.