Notice: this document is an unofficial translation of the Swedish Authority for Privacy Protection´s (IMY) final decision in case with national refernce number, DI-2021-9842. Only the Swedish version of the decision is deemed authentic.

Registration number:
DI-2021-9842

Date:
2023-08-03

Decision under the General Data Protection Regulation- Jollyroom AB

Decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection (IMY) finds that Jollyroom AB (556815-7159) has processed the complainant's personal data in breach of Article 32(1) of the General Data Protection Regulation (GDPR)[1] by failing to take appropriate technical and organisational measures to ensure adequate protection against unauthorised disclosure on its website for personal data in the complainant's customer profile.

The Authority for Privacy Protection issueJollyroom ABa reprimand pursuant to Article 58(2)(b) of the GDPR for the infringement of Article 32(1) of the GDPR.

Report of the supervisory report

Handling

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding Jollyroom AB due to a complaint. The complaint has been submitted to IMY, as lead supervisory authority under Article 56 GDPR. The handover has been made by the supervisory authority of the country where the complainant has lodged his complaint (Denmark) in accordance with the Regulation's provision on cooperation in cross-border processing.

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

The complaint

It is stated in the complaint that on 6th of November 2019 there was a security flaw on Jollyroom AB's danish website. The complainant has observed that it was possible for him to log in to Jollyroom's customer service function using only email and zip code.

[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).

Mailing address:
Box 8114
104 20 Stockholm
Website:
www.imy.se
E-mail:
imy@imy.se
Phone:
08-657 61 00

There was therefore no need for a password or other identification method for logging in. After the complainant has logged in with the new method, he could see the individual's profile including; name, e-mail, telephone number and address.

What Jollyroom AB has stated

Jollyroom AB has mainly stated the following.

The company is the controller for the processing to which the complaint relates.

The complainants description is true in all relevant aspects. The incident has been a consequence of a bug in the system and has not been a deliberate implemented functionality on the website. Due to unforeseen technical problems, the functionality ended up outside the general customer profile logic with login requirements. The functionality was intended for those who were logged in to their customer profiles. This functionality was implemented unintentionally and has not allowed access to the entire customer profile, but only to the following categories of data. Name, email address, telephone number, address, postcode and postal location. This security flaw has not given access to all the categories of data available in regular logged-in mode, thus no order history has been exposed.

The company's website incorporates other commonly used security mechanisms such as password requirements for access to customer data and encrypted transport protocols for data traffic.

The current system has been replaced.

Justification of the decision

Applicable provisions

Article 32 regulates the security of the processing. Paragraph 1 requires the controller, taking into account the latest developments, the costs of implementation and the nature, scope, context and purpose of the processing as well as the risks, of varying probability and severity, to the rights and freedoms of natural persons, to take appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

According to Article 32(2), when assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, the personal data transmitted, stored or otherwise processed.

Assessment of the Authority for Privacy Protection (IMY)

IMY notes, first of all, that Jollyroom AB, has taken steps to ensure that the individual's data are now password protected.

However, IMY has found that the exposure of the complainant's personal data was possible through its non-intentional functionality, the complainant's personal data did not have sufficient protection against unauthorised disclosure. In IMY's assessment, the lack of adequate protection should have been discovered before the controller started processing personal data. IMY considers that Jollyroom AB has not taken

appropriate technical and organisational measures pursuant to Article 32(1) to ensure adequate protection against unauthorised disclosure on its website for personal data in the complainant's customer profile. Jollyroom AB has thus processed personal data in breach of Article 32(1) of the General Data Protection Regulation.

Choice of intervention

It follows from Article 58(2) of and Article 83(2) of the GDPR that 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 is the aggravating and mitigating circumstances in the case, such as the nature, gravity and duration of the infringement and past relevant infringements.

IMY notes the following relevant facts. The supervision covers the processing of an individual complainant's personal data in the situation to which the complaint relates. The infringement was committed negligently. Neither sensitive nor integrity-sensitive data have been involved. Furthermore, the company has taken measures to protect information against unauthorised disclosure. IMY has not previously established that the company has infringed the GDPR.

Against this background, IMY considers that it is a minor infringement within the meaning of recital 148 and that Jollyroom AB should be reprimanded pursuant to Article 58(2)(b) GDPR.

This decision has been taken by Acting Head of Unit for [redacted] after a presentation by the legal expert [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.