Avanza Bank AB
Regeringsgatan 103
111 39 Stockholm

File number:
DI-2021-5544

Date:
2024-06-24

Decision following supervision under the General Data Protection Regulation against Avanza Bank AB

Decision of the Data Protection Authority

The Swedish Data Protection Authority finds that Avanza Bank AB (company registration number 556573-5668) has processed personal data in violation of Articles 5(1)(f) and 32(1) of the General Data Protection Regulation[1] by not having taken appropriate technical and organisational measures to ensure an adequate level of security for personal data during the period from 15 November 2019 to 2 June 2021 when using the Meta-pixel analysis tool.

Pursuant to Articles 58(2) and 83 of the GDPR, the Swedish Data Protection Authority decides that Avanza Bank AB shall pay an administrative fine of SEK 15,000,000 (fifteen million) for the infringements of Articles 5(1)(f) and 32(1) of the GDPR.

Description of the enforcement case

Starting point for supervision

On 8 June 2021, the Swedish Authority for Privacy Protection (IMY) received a notification of a personal data breach from Avanza Bank AB (the bank). The notification stated that personal data of 500,001 - 1 million during the period from 15 November 2019 to 2 June 2021 inclusive was incorrectly transferred to the bank's partner Facebook (now Meta). The data transferred included personal identity numbers, loan amounts and account numbers.

The background to the incident was that the bank had started using Meta's Facebook pixel service (now the Meta pixel) in order to optimise the bank's marketing. In 2019, Meta developed a new sub-function within the Meta pixel, called Automatic Advanced Matching (AAM). The erroneous transfer of personal data was caused by the new AAM feature being activated by the bank by mistake. The bank became aware of the transfer via external information. As soon as the bank became aware of the incident, it deactivated the Meta-Pixel in its entirety.

[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 the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Based on the information contained in the breach notification, IMY initiated an inspection of the bank. The supervision has been limited to the extent to which the bank has taken appropriate technical and organisational measures to protect the personal data of website visitors and app users in accordance with Articles 5(1)(f) and 32(1) of the GDPR during the period from 15 November 2019 to 2 June 2021.

What the bank has stated

The Bank has essentially stated the following regarding the issues under review by the IMY.

Personal data liability

The Bank is the controller for the implementation of the Meta-Pixel and the subsequent transfer of personal data to Meta.

The original implementation of the Meta-pixel

The Bank has procedures in place to ensure the correct processing of personal data before, in connection with and after the introduction of new features on the website. These procedures are formalised and documented in the bank's governing documents. According to the bank's procedures for ensuring the correct processing of personal data, a review and assessment of the planned processing must be carried out initially before any new or changed personal data processing to ensure that it meets the requirements of the General Data Protection Regulation. The review is done using, among other things, a documented template for personal data processing, which contains a number of steps that the employee responsible for the introduction of a new or changed personal data processing must go through. The steps include conducting a risk analysis of the processing, establishing a legal basis and ensuring that the data subjects are given correct information about the new personal data processing. Furthermore, the processing must be entered in the bank's register.

The Meta-Pixel is an analytics tool provided by Meta that helps measure the effectiveness of the bank's Facebook advertising. The Meta pixel transmitted and linked the activity and behaviour of a website visitor on the bank's website to a unique registered user of one of Meta's services. The purpose of introducing and using the Meta pixel was to optimise the bank's marketing.
The purpose of the processing of personal data was to use targeted advertising on Facebook and to market the bank to a relevant target group. The meta-pixel enabled more relevant marketing to be produced by basing the marketing on information about which pages on the bank's website a person visited.

Before the bank started its co-operation with Meta, an approval process was carried out involving the bank's risk, compliance, legal and information security functions. Within this process, issues of banking secrecy and personal data processing were addressed. The only data that needed to be processed for this purpose was information on the web pages visited by an individual, the IP address, and information on certain unique events, such as product selections and website searches.

Activation of new Meta-pixel sub-functions

In 2019, Meta developed the Meta-Pixel service by also providing the Automatic Advanced Matching ("AAM") function. This is a sub-function within the Meta-pixel. In addition to AAM, the Meta pixel also offers the Automatic Events ("AH") function, which can be activated manually and which then tries to detect and capture events and interactions, such as clicks, searches and menu selections, when visiting the company's website or app.

In 2019, the bank's legal department received an enquiry from the marketing department about the possibility of using one of Meta's functions through which customer data would be transferred to Meta. The bank's legal department found that the function in question could not be implemented. Furthermore, it is the bank's view that if the implementation of a function such as AAM had been subject to internal processes and procedures, this would have led to the assessment that the bank would not have been able to accept the terms and conditions and that it would not be possible to use the function. This is because the function risks entailing a transfer of data to Meta that the bank cannot legally perform in its banking operations.

It was never the bank's intention to use the AAM and AH functions, and the bank has not been able to verify how the functions were activated. If the function was activated by a bank employee, the bank's view is that it was done by mistake. The bank has not taken any decision to activate the AAM function.

Transfer of personal data by the Bank via the AAM function to Meta

Automatic Advanced Matching (AAM) functions

The AAM function transmitted data in hashed form (using the SHA256 hashing function)[2] to Meta if the user filled in any of the five different forms on the bank's website or mobile app. Two forms were in the new customer flow (open to visitors, where the visitor intended to become a customer). Three forms related to mortgages and were behind login and could only transfer data from existing customers who had signed a customer agreement with the bank. Thus, in order for the data to be transferred, a person had to be logged in to the bank's website and to have accepted the bank's marketing cookies. If these conditions were not met, the AAM was not activated and no data was transferred. If the conditions were met, the following hashed data could be transferred to Meta:

- Personal identification number
- Contact details, such as phone number, email address, postcode and post town
- Loan amount on existing loan
- Employers
- Type of employment
- Account number

[2] IMY addendum: Hashing is a one-way cryptographic function that can be used to achieve pseudonymisation, which is a possible security measure under Article 32 of the GDPR, by replacing personal data with a so-called hash sum. This means that the replaced personal data is not available in plain text and that additional information is needed to identify the data subject.

The inadvertent activation of the AAM feature by the bank allowed the Meta-Pixel to match the hashed data with the behaviour of visitors to the website for profiling purposes.
This made it possible to obtain a more detailed picture of visitors. The profiling was for marketing purposes only and was not used by Meta for its own, or other organisations', commercial purposes.

The exact impact of AAM on advertising has not been established. That this has resulted in targeted advertising cannot be excluded.

Automatic Events (AH) function

The AH function transmitted data in plain text to Meta when a user navigated the bank's website or mobile app. A prerequisite for transmission was that the user had accepted the bank's marketing cookies and was logged in as a customer of the bank (with one exception, see below).

The data transmitted in plain text to Meta was transmitted unconsciously as there was no intention to show the information to anyone other than the customer. It was from the browser or app on the customer's device that the transfer took place, due to three main factors:

1) The function inadvertently activated by the bank at Meta also tracks how a user moves around a site/mobile phone (converts). To do so, it sends information about which "buttons" - that is, elements on the page/screen - the user presses when navigating the site/app. Meta thus collects information that tells it which button presses occur in order to understand the context in which the user is converting. For example, Meta wants to understand that the customer buys something when pressing a button with the text "Buy" even if the advertiser has not tagged the buy button as a conversion. This information was sent to Meta.

2) The bank uses elements that Meta perceives as buttons, such as button-marked boxes and drop-down menus, in its code to present certain information to the bank's users. This is mainly the case when there are elements on the site/apps that can be pressed to display more information, for example. Often these are displayed as a smaller visual element that becomes larger when tapped, showing more information. When users have pressed these elements to see more information, it has been recorded as regular button presses by Meta's script (Meta pixel IMY's note). The script has then compiled the information and sent it to Meta as a registered button press.

3) Button press information is not pseudonymised (hashas IMY's note) by Meta in the same way as other information they collect.

These three factors combined to send some information to Meta in plain text. Thus, it was a combination of the (wrongly) activated functionality together with Meta's button press handling and a specific technical solution from the bank that caused the transmission to Meta.

In summary, AH analysed which buttons on the website and mobile app were pressed by the user in order to provide marketing suggestions on Facebook. The bank's transfer of data via AH occurred because the bank categorised visual fields as buttons on the website and in the mobile app code. Via AH, the following categories of data could be transmitted to Meta in plain text:

- Securities holdings and value, such as amount available for purchase, withdrawal and performance
- Information on loan amounts
- Account number and credit limit
- Fees, taxes and current interest rates
- Orders in progress and end of day
- Signatory and bank as pension moved from
- E-mail address and social security number

The majority of the data transmitted via the AH came from buttons behind the bank's login, i.e. buttons that were only visible to customers who had signed a customer agreement with the bank. However, at one point on the bank's website, there were expandable panels in the flow for taking out occupational pensions, both for sole traders and for limited companies, which were open to all visitors, i.e. also data from a limited number of visitors without a customer agreement with the bank and who were therefore not logged in.

Actions taken following the personal data breach

Meta has confirmed to the Bank that the personal data processed has been deleted at Meta in a way that does not allow Meta to recover it.

The bank's view is that the transfer of the data did not entail any harm or risk to the data subjects, as Meta did not use the data for its own purposes or transfer it further, and the data has been deleted. All data has been transferred by the Meta pixel to Meta and the bank's own advertising account with Meta.

In order to detect outgoing traffic, the bank has now established a process for how it implements and manages third-party scripts. It describes how these scripts are to be evaluated from a security and privacy perspective and how they are maintained in the long term.

Furthermore, the bank has moved the scripts from the third-party providers to the bank's own systems to avoid changes to the scripts being introduced without the bank's knowledge.

The bank has also completed internal guidelines to more clearly describe the failure scenario, how it is avoided and the expectations of the bank's development team when dealing with this type of product.

In addition, the Bank has implemented further policies and procedures aimed at ensuring the proper processing of personal data. These policies include requirements and guidelines in relation to the processing of personal data before, during and after the introduction of new features on the Bank's website.

Reasons for the decision

Applicable provisions etc.

It follows from Article 95 of the GDPR that the GDPR shall not impose any additional obligations on natural or legal persons processing personal data, for areas already covered by obligations according to the so-called eData Protection Directive[3] . The eData Protection Directive has been implemented in Swedish law through the Electronic Communications Act (2003:389), which regulates, among other things, the collection of data through cookies.

According to Chapter 9, Section 28 LEK, which implements Article 5(3) of the ePrivacy Directive, data may be stored in or retrieved from a subscriber's or user's terminal equipment only if the subscriber or user is provided with information about the purpose of the processing and consents to it. Furthermore, it is clear that this does not prevent storage or access that is necessary for the transmission of an electronic message over an electronic communications network or that is necessary for the provision of a service explicitly requested by the user or subscriber. LEK entered into force on 22 August 2022. However, during the period in question, the same requirements applied under Chapter 6, Section 18 of the Electronic Communications Act (2003:389). It is Post- och telestyrelsen, which is the supervisory authority under LEK (Chapter 1, Section 5 of the Electronic Communications Ordinance (2022:511)).

The European Data Protection Board (EDPB) has issued an opinion on the interaction between the ePrivacy Directive and the GDPR. The opinion states, inter alia, that the national supervisory authority designated under the ePrivacy Directive is solely competent to monitor compliance with the Directive. On the other hand, the supervisory authority under the GDPR is the competent supervisory authority for processing not specifically regulated by the ePrivacy Directive.[4]

According to Article 4(7) of the GDPR, the controller is a natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data. Where the purposes and means of processing are determined by Union or Member State law, Union or Member State law may provide for the controller or the specific criteria for its designation.

The controller is responsible for and must be able to demonstrate compliance with the basic principles of Article 5 of the GDPR. This is set out in Article 5(2) of the GDPR (accountability principle).

Article 5(1)(f) of the GDPR requires personal data to be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 32(1) of the GDPR requires the controller to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk represented by the processing. In assessing the appropriateness of the technical and organisational measures, the controller shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks to the rights and freedoms of natural persons.

[3] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[4] Opinion 5/2019 on the interaction between the Directive on privacy and electronic communications and the General Data Protection Regulation, in particular as regards the competences, tasks and powers of data protection authorities, adopted on 12 March 2019, paragraphs 68 and 69.

According to Article 32(1), appropriate safeguards include, where appropriate,

a) pseudonymisation and encryption of personal data,
b) the ability to ensure the confidentiality, integrity, availability and resilience of processing systems and services on an ongoing basis,
c) the ability to restore availability and access to personal data in a reasonable time in the event of a physical or technical incident; and
d) a procedure to regularly test, examine and evaluate the effectiveness of the technical and organisational measures to ensure the security of processing.

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

According to Chapter 3, Section 10 of the Act (2018:218) with supplementary provisions to the EU General Data Protection Regulation, personal identity numbers and coordination numbers may be processed without consent only when it is clearly justified with regard to the purpose of the processing, the importance of secure identification or some other noteworthy reason.

Chapter 1, section 10, first paragraph of the Banking and Financing Business Act (2004:297) states that individuals' relationships with credit institutions may not be disclosed without authorisation.

The assessment of the Data Protection Authority

The investigation in the case shows that two functions in the Meta pixel analysis tool were inadvertently activated by the bank. As a consequence of the activation of the functions, personal data about a large number of people who were logged in to the bank's website or app was unauthorisedly transferred to Meta. In some cases, personal data relating to individuals who visited the website or app and used a specific service without being logged in was also transferred. The transfers mainly concerned the bank's own customers. The personal data transferred has included, among other things, personal identification numbers and extensive financial information. In several cases, the information, including detailed customer financial data, was transferred in plain text.

According to the bank, it has not been possible to verify ex post how the functions were activated or by whom.

IMY initially considers whether the GDPR applies and whether IMY is the competent supervisory authority.

IMY is the competent supervisory authority

IMY's review focuses on a situation where data of individuals, mainly customers logged in to the bank, were inadvertently transferred by the Meta-Pixel to Meta when they visited different parts of the bank's website. This information processing does not involve data being stored in or retrieved from a subscriber's or user's terminal equipment and is therefore not covered by
Chapter 9, section 28 of LEK or the previously applicable corresponding provision in the Electronic Communications Act (2003:389). IMY thus concludes that the GDPR is

applicable to the personal data processing in question and that IMY is the competent supervisory authority. It can also be noted that IMY's review concerns whether the bank has taken sufficient security measures, which is not something that is specifically regulated in the LEK. This fact also means that IMY is the competent supervisory authority.

IMY then assesses the issue of data liability and whether the Bank has taken appropriate safeguards under Articles 5(1)(f) and 32 of the GDPR to protect the personal data of the website visitors and app users concerned.

The bank is the data controller

The bank has stated that it is the controller for the personal data processing examined in the case. The investigation shows that the purpose of implementing and using the Meta pixel was to optimise the bank's marketing. By processing data on, for example, a person's visited web pages, searches and product choices, the bank's marketing on Meta's Facebook service has thus been optimised.

IMY notes that the bank has determined the purposes and means of the processing of personal data, i.e. how and why the personal data is to be processed. IMY assesses that the bank is the controller of the personal data processing covered by the supervision in accordance with Article 4(7) of the GDPR.

The treatment has involved a high risk and required a high level of protection

The Bank has an obligation under Article 32 of the GDPR to protect the personal data it processes by implementing appropriate technical and organisational measures. These measures shall ensure an appropriate level of security. In assessing the appropriate level of security, the controller shall take into account the costs, nature, scope, context and purposes of the processing and the risks to the rights and freedoms of natural persons that the processing entails.

Chapter 1, section 10, first paragraph of the Banking Act states that a person who is or has been associated with a bank may not unauthorisedly disclose information concerning a bank customer's dealings with the bank. The information that a particular person is or is not a customer of the bank is also covered by the duty of confidentiality. These legal requirements on professional secrecy thus apply to the bank's operations. This places high demands on the protection of the personal data processed in the bank's operations.

The IMY notes that the data processed included personal data requiring special protection, namely personal identification numbers, which may only be processed under certain conditions. It has also involved financial data, such as account numbers, securities holdings, loan amounts, and credit limits, for which data subjects have a legitimate expectation of a high degree of confidentiality and robust protection against unauthorised access. The data transferred have been subject to legal professional secrecy. The processing of personal data has taken place in the context of the Bank's core business, which places even higher demands on the level of protection. The bank should have been able to ensure a level of security appropriate to the scope and sensitivity of the processing.

In view of the fact that the data processed by the bank was of a sensitive nature and concerned a very large number of people, the bank's processing of the personal data involved a high risk for natural persons rights and freedoms. The nature, scope and context of the processing therefore required a high level of data protection. The measures were to ensure, inter alia, that the personal data were protected against unauthorised disclosure and access.

The bank has not taken sufficient measures to protect the data

As a preliminary remark, IMY notes that the fact that the bank transferred the data in question to Meta means that the data were not in fact protected against unauthorised disclosure.

The information provided by the bank shows that it has formalised procedures to ensure the correct processing of personal data before, during and after the introduction of new features on the website and that these procedures are documented in the bank's governing documents.

IMY notes that the bank thus had organisational measures in place in the form of procedures documented in the bank's governing documents. However, in this case the bank has not followed its procedures. The bank has had the Meta pixel implemented on parts of the bank's website and app that were intended only for logged-in customers and potential customers. The two functions AAM and AH in the Meta-pixel were subsequently activated without the bank being aware of this. As a consequence of the bank not following its procedures and documenting what happened when these functions were introduced, it has not been possible for the bank to subsequently verify how or by whom these functions were activated.

As a result of the activation of the two functions AAM and AH without the Bank's knowledge, there was an unauthorised disclosure of information covered by professional secrecy and an unauthorised transfer of personal data to Meta. This went on for over a year and a half. The cessation of the disclosure and unauthorised transfer was not due to the bank itself becoming aware of what was going on, but to the bank becoming aware of it via an external source.

The bank has thus lacked the ability to detect the disclosure and ongoing transfer of personal data to Meta. IMY is of the opinion that the bank should have had such a systematic security programme that this would have been detected by the bank. Such security work includes that checks are made with some regularity. Since the bank has only had procedures for following up documented changes carried out in accordance with established procedures, the bank has lacked the ability to detect and rectify changes which, as in the present case, have been carried out without following the procedures. Against this background, IMY concludes that the bank has lacked technical and organisational security procedures to systematically follow up and detect unintentional changes in its systems.

As a result of the bank's failure to apply its organisational security procedures when the bank introduced the AAM and AH functions, and the lack of organisational and technical security procedures to detect transfers, personal data on a large number of individuals was transferred to Meta without authorisation. The investigation shows that the personal data of approximately 500,000 - 1,000,000 individuals were transferred.

In summary, IMY concludes that the bank did not take sufficient technical and organisational measures to ensure a level of security appropriate to the risk when using the Meta-pixel. This means that the bank during processed personal data in breach of Article 32(1) of the GDPR between 15 November 2019 and 2 June 2021.

According to the basic security principle of Article 5(1)(f) of the GDPR, personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. As a result of the incident, data on the bank's customers, such as personal identification numbers, account numbers, securities holdings, loan amounts and credit limits, have been transferred to Meta in plain text.
In addition, some data have been transferred in hashed form, which enabled matching with personal data at Meta. This has been data that is subject to statutory confidentiality. Loss of control of banking information can pose a high risk to the rights and freedoms of data subjects. According to IMY, the fact that the case concerns banking information and that the personal data has also been predominantly disclosed and transmitted in plain text from a logged-in mode for customers means that the incident is particularly serious. The bank's failure to follow its formalised procedures and lack of ability to detect the unauthorised transfer of personal data is therefore deemed to be of such a serious nature that the deficiency also constitutes a breach of Article 5(1)(f) of the GDPR.

Choice of intervention

Legal regulation

IMY has a number of remedial powers in the event of infringements of the GDPR, including reprimands, injunctions and penalties. This follows from Article 58(2)(a) to (j) of the GDPR. IMY shall impose penalties in addition to or instead of other corrective measures referred to in Article 58(2), depending on the circumstances of each case.

Each supervisory authority shall ensure that the imposition of administrative fines in each individual case is effective, proportionate and dissuasive. This is set out in Article 83(1) of the GDPR.

Article 83(2) sets out the factors to be taken into account in determining whether an administrative penalty should be imposed and what may affect the amount of the penalty. Factors relevant to the assessment of the seriousness of the offence include its nature, gravity and duration.

Article 83(4) provides that administrative fines of up to EUR 10 000 000 or, in the case of an undertaking, up to two per cent of the total worldwide annual turnover in the preceding financial year, whichever is the higher, shall be imposed for infringements of, inter alia, Article 32.

Article 83(5) provides that administrative fines of up to EUR 20 000 000 or, in the case of an undertaking, up to 4 % of its total worldwide annual turnover in the preceding financial year, whichever is the higher, shall be imposed for infringements of, inter alia, Article 5.

The EDPB has adopted Guidelines on the calculation of administrative fines under the GDPR which aim to create a harmonised methodology and principles for the calculation of administrative fines.[5]

In the case of a minor infringement, IMY may issue a reprimand under Article 58(2)(b) of the Regulation instead of imposing a financial penalty, as explained in recital 148.

IMY's assessment

The penalty shall be imposed

IMY has concluded that the bank has processed personal data in breach of Article 32(1) of the GDPR and that the breach is of such a serious nature that it also constitutes a breach of the principles of integrity and confidentiality in Article 5(1)(f).

The breach occurred because the bank processed personal data with an inadequate level of security, which resulted in, among other things, the unauthorised transfer of financial data on approximately 500,000 - 1,000,000 individuals to Meta over a period of more than one and a half years. Furthermore, the bank has lacked the ability to detect the transfer of personal data to Meta during this time. IMY is of the opinion that the bank should have had such systematic security work that the transfer of personal data would have been detected in connection with a regular control. The unauthorised transfer has resulted in a high risk to the rights and freedoms of data subjects, including loss of confidentiality of data worthy of protection. Against this background, IMY considers that this is not a minor infringement as referred to in recital 148 of the GDPR.

The CJEU has clarified that the imposition of administrative fines under the GDPR requires that the controller has committed an infringement intentionally or negligently. The CJEU has ruled that controllers can be fined for behaviour if they cannot be considered to have been unaware that the behaviour constituted an infringement, regardless of whether they were aware that they were breaching the provisions of the GDPR.[6]

According to the principle of accountability expressed, inter alia, in Article 5(2) of the GDPR, the party responsible for the processing of personal data must ensure and be able to demonstrate that the processing complies with the GDPR. IMY thus notes that the bank is responsible for ensuring that the personal data processed in its operations are processed in a manner that ensures an appropriate level of security. IMY has found that the bank has not complied with the requirements of the GDPR in this regard. The bank cannot be considered to have been unaware that its behaviour constituted an infringement of the Regulation. The

[5] EDPB Guidelines Guidelines 04/2022 on the calculation of administrative fines under the GDPR, adopted on 24 May 2023.

[6] Judgment of the Court of Justice of the European Union in Case C-683/21 Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos
v Valstybinė duomenų apsaugos inspekcija of 5 December 2023, paragraph 81 and
judgment in Case C 807/21 Deutsche Wohnen of 5 December 2023, paragraph 76

there are therefore grounds for imposing an administrative penalty on the bank.[7]

When determining the amount of the administrative fine, the IMY shall take into account the circumstances set out in Article 83(2) and shall ensure that the administrative fine is effective, proportionate and dissuasive.

The IMY notes that infringements of Article 5(1)(f) of the GDPR fall within the scope of Article 83(5), which allows for the imposition of a fine of up to EUR 20 million or 4 per cent of the global annual turnover of the preceding financial year, whichever is higher.

The Avanza Group's annual turnover according to the parent company's consolidated accounts shall be used as the basis for the calculation

In determining the maximum amount of a fine to be imposed on an undertaking, the definition of an undertaking used by the Court of Justice of the European Union for the purposes of Articles 101 and 102 TFEU (see recital 150 of the GDPR) should be applied. It follows from the case-law of the Court that this includes any entity engaged in an economic activity, regardless of its legal form and the way in which it is financed and even if the entity is legally composed of several natural or legal persons.

The assessment of what constitutes an undertaking should therefore be based on competition law definitions. The rules on group liability in EU competition law revolve around the concept of economic unit. A parent company and a subsidiary are considered part of the same economic entity when the parent company exercises decisive influence over the subsidiary. The decisive influence (i.e. control) can be achieved either by ownership or by contract. Case law shows that 100 per cent or almost 100 per cent ownership creates a presumption of control. However, the presumption can be rebutted if the undertaking provides sufficient evidence to prove that the subsidiary acts independently on the market.[8] Thus, in order to rebut the presumption, the undertaking must provide evidence concerning the organisational, economic and legal links between the subsidiary and its parent company showing that they do not form an economic unit despite the fact that the parent company holds 100% or almost 100% of the shares.[9]

Avanza Bank AB is a wholly owned subsidiary of the parent company Avanza Bank Holding AB (publ). According to the presumption described above, it is therefore the turnover of the Avanza Group according to Avanza Bank Holding AB's (publ) consolidated accounts that shall be used as the basis for calculating the maximum amount of the administrative fine.

Avanza Bank Holding AB's consolidated financial statements for 2023 show that the total global annual turnover was approximately SEK 4,716,000,000. Four per cent of that annual turnover is approximately SEK 189 000 000. As this amount is below the maximum amount set out in Article 83(5), the maximum penalty that can be imposed in this case is EUR 20 000 000.

[7] For the assessment of negligence, see also the judgment of the Administrative Court of Appeal in Stockholm of 11 March 2024 in Case 2829-23, p. 12.

[8] Judgment of the Court of Justice of the European Union in Case C-97/08 P Akzo Nobel NV and others v Commission of the European Union, 10 September 2009, paragraphs 59-61 Adapt/add footnotes where we refer to the CJEU rulings.

[9] Cf. EDPB Guidelines 04/2022 on the calculation of administrative fines under the GDPR, paragraph 125 and the decisions cited therein.

Gravity of the offence

The EDPB Guidelines state that the supervisory authority should assess whether the infringement is of low, medium or high seriousness.[10]

IMY considers that the following factors are relevant to the assessment of the gravity of the infringement.

IMY has found that the bank did not follow its procedures in connection with the activation of the AAM and AH functions in the Meta pixel and that the bank lacked the systematic security work required to detect the unauthorised disclosure and transfer of personal data to Meta. The security breaches in question have led to an incident that has affected a large number of data subjects and Meta has been able to access a large amount of personal data, in many cases in plain text, that should not have been transferred to Meta.
The data included financial and social security number data, i.e. data requiring a high level of protection. The breach has been ongoing for a long period of time, from 15 November 2019 until 2 June 2021, when the bank became aware of the unauthorised transfer of the data. The processing of the personal data on the Bank's website is part of the Bank's core business where the data was subject to a legal obligation of professional secrecy, which makes the breach more serious than if this had not been the case.[11]

IMY has concluded that the infringement is so serious that, in addition to a breach of Article 32(1) of the GDPR, it also constitutes a breach of the fundamental principle of privacy and confidentiality under Article 5(1)(f).

In assessing the amount of the fine, IMY shall also take into account the aggravating and mitigating factors listed in Article 83(2) of the GDPR. IMY notes that the Bank took certain measures to mitigate the damage suffered by data subjects under Article 83(2)(c). The bank immediately switched off the pixel features when it was made aware of the transfer. The bank also contacted Meta to ensure that Meta did not process the data for its own purposes and that the data was deleted at Meta. In addition to this, the bank has implemented further policies and procedures aimed at ensuring the correct processing of personal data. IMY assesses that through these measures the bank has done what could be expected given the nature, purpose and scope of the processing. Therefore, the measures taken do not constitute a mitigating factor. IMY notes that no other circumstances have emerged that affect IMY's assessment of the size of the fine, either in an aggravating or mitigating direction

The penalty must be effective, proportionate and dissuasive

The administrative fine must be effective, proportionate and dissuasive. This means that the amount must be determined in such a way that the administrative fine leads to rectification, that it has a preventive effect and that it is also proportionate to both the offences concerned and the supervised entity's ability to pay.

[10] EDPB Guidelines 04/2022 on the calculation of administrative fines under the GDPR, point 60.
[11] EDPB Guidelines 04/2022 on the calculation of administrative fines under the GDPR, paragraph 53.

In view of the gravity of the infringement, IMY decides that the bank shall pay an administrative fine of SEK 15 000 000 for the infringements found. IMY considers that this amount is effective, proportionate and dissuasive.

This decision was made by the Acting Director General, David Törngren, after a presentation by senior lawyer Hans Kärnlöf. Acting Head of Legal Affairs Cecilia Agnehall, Head of Unit Catharina Fernquist and IT and information security specialist Petter Flink also participated in the final processing.

David Törngren, 2024-06-24 (This is an electronic signature)

Copy to
DSO

How to appeal

If you want to appeal the decision, you should write to the Data Protection Authority. In your letter, please specify the decision you are appealing and the change you are requesting. The appeal must be received by the Authority no later than three weeks from the date you received the decision. If the appeal has been received in time, the Authority will forward it to the Administrative Court in Stockholm for consideration.

You can e-mail the appeal to the Authority if it does not contain any privacy-sensitive personal data or data that may be subject to confidentiality. The contact details of the Authority can be found on the first page of the decision.