

Complainant

See Annex

Subject of the investigation

Boozt Fashion AB
Box 4535
203 20 Malmö

Registration number:

DI-2020-10540

Date:

2024-01-04

Final decision pursuant to Article 60 under the General Data Protection Regulation – Boozt Fashion AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection finds that Boozt Fashion AB (556710-4699) has processed the complainant's¹ personal data in breach of:

- Article 6 (1) of the General Data Protection Regulation (GDPR)² by, at the time of the request for erasure on the 28 November 2019, having continued to process the complainant's personal data for the purpose of prevention of misuse of services and fraud without being able to demonstrate a legal basis for the processing.
- Article 12(1) and (3) and Article 15(1) by within one month neither having complied with the complainant's request for access to her personal data of 30 January 2020 nor having informed the complainant in writing of the delay and not having provided the information in a transparent form; and
- Article 12(4) by providing, in reply of 23 December 2019 to the complainant's request for erasure pursuant to Article 17 of 28 November 2019, incorrect information that all data had been deleted and did not inform about the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

The Swedish Authority for Privacy Protection issues a reprimand to Boozt Fashion AB pursuant to Article 58(2)(b) of the GDPR for the infringement of Articles 6 (1), 12(1), 12(3), 12(4) and 15(1).

Pursuant to Article 58(2) (d) of the GDPR, the Swedish Authority for Privacy Protection orders Boozt Fashion AB to ensure that the information about the complainant that the company collected and processed at the time of the request for erasure on the 28 November 2019 for the purpose of preventing misuse of services and fraud are no

Mailing address:

Box 8114
104 20 Stockholm

Website:

www.imy.se

E-mail:

imy@imy.se

Phone:

08-657 61 00

^{1 1} The complainant's identification data are set out in Annex.

² 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 celebrating the movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

longer processed for that purpose, and inform the complainant of those measures in accordance with Article 12(3). The measures shall be implemented no later than two weeks after this decision becomes legally binding.

Presentation of the supervisory case

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding Boozt Fashion AB (hereinafter Boozt 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 GDPR. The handover has been made by the supervisory authority of the country where the complainant has lodged her complaint (Denmark) in accordance with the provisions of the GDPR on cooperation in cross-border processing.

The case has been handled through written procedure. In the light of the complaint relating to 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 Denmark, France, Italy, Norway, Germany, Austria, Finland, Poland and Spain.

The complaint

The complaint states, *first*, that the company partially refused to comply with the complainant's request for erasure of her personal data. Furthermore, that the company stated to the complainant that the complainant's personal data is needed for (1) accounting purposes, (2) handling complaints and (3) defence of legal claims. In addition, the complainant states that the company has claimed that data is necessary for (4) prevention of misuse of services and fraud, since the company considers that the complainant misused the company's business offer by returning too many orders over a 12-month period and was therefore blocked from making further purchases in accordance with the company's Fair Use policy. The complainant challenges the legality of the Boozt Fair Use policy by claiming that it undermines and circumvents the consumer's statutory right of withdrawal within 14 days.

Secondly, the complainant requested for access to her data on 30 January 2020. The company did not give the complainant access to the data until 25 March 2020, that is to say, about two months after the request was made, without prior notification of the delay. Furthermore, the information provided to the complainant at that time was not complete, in any event personal data were missing in e-mail correspondence.

What Boozt has stated

Boozt has mainly stated the following.

Request for erasure and the company's communication log

The company received two requests for erasure from the complainant, on 28 November 2019 and 18 January 2020. On 30 December 2019, the complainant also objected to the company's processing of her personal data in order to maintain a blocking of the complainant's attempts to purchase, on the basis of the company's Fair Use policy.

The request for erasure has been dealt with in accordance with the company's normal procedure. This means that after a request has been received, a confirmation is sent

with information that an email has been sent to the current email address of the data subject to confirm that the request has been made by the authorised person and that when authorisation is confirmed, erasure will begin.

The complainant's request for erasure was complied with in so far as it considered it to be obliged to do so. This includes the termination of direct marketing (based on history, favorites and cookies) and email conversations with the complainant that were not deemed necessary for ongoing processing operations, including the complainant's requests for erasure and confirmation that erasure has been carried out. After the erasure of those data, only traces of the current handling of the complainant's requests can be found in the company's communication log.

Boozt observes that the information provided to the complainant on 23 December 2019 wrongly gave it the view that the information underlying the Fair Use policy should also be deleted. The company sought to rectify this by subsequent communication with the complainant on 30 December 2019.

Boozt has kept information that the request for erasure was made and information that the complainant's identity was confirmed by clicking on a link in the e-mail that expired from the company. For each event, the communication log shows a unique event ID, the complainant's e-mail address, a time stamp, a description of the event, possibly the order number, the status of the event, any shopping basket number, and the date and time.

The communication log itself is only a means of the processing of personal data included in Boozt processing for the purpose of demonstrating accountability in Article 5(2) and Article 24. The data may also be used in defence of legal claims, in parallel proceedings with the complainant and also with the legal basis of legitimate interest. The data will be processed for as long as the legitimate reasons remain in the light of the processes and its timeframes, provided that the interests or fundamental rights and freedoms of the data subject do not outweigh the interests or fundamental rights and freedoms of the data subject.

In addition to the procedure in place at the time of the complainant's request for erasure, Boozt considers that it has not retained sufficient data to comply with the liability of the GDPR regarding the demonstration of how the complainant's requests are handled. That is because the company deleted the complainant's data in response to the request for erasure of 28 November 2019 and thus failed to demonstrate that there was any confirmation that the erasure had been carried out.

Boozt has now drawn attention to the fact that automatic erasure when requesting erasure, as the function has been structured, has adversely affected Boozt's ability to demonstrate compliance with liability. Boozt also continuously trains its Customer Service agents (and other) staff in terms of data subjects' rights, Boozt obligations and practical lessons as they are made.

Request for access

Boozt provided a copy of the complainant's information in response to the complainant's request for access of 30 January 2020 pursuant to Article 15, but, in its own assessment, did not comply with the requirement of transparency in relation to the request.

As regards *information*, on 25 March 2020, the complainant obtained access to a copy of direct extracts of the data relating to the complainant contained in the Boozt system at that time. Furthermore, the Complainant obtained through the attached Personal Data Policy and Cookie Policy in accordance with Article 15(1)(a) to (h) a description of the processing operations to which the data belonged, (2) information on the origin and purpose of these data, (3) data on recipients or categories of recipients, (4) where relevant, information on the anticipated period during which the personal data will be stored or the criteria used to determine this period, (5) the existence of the right to request rectification or erasure of the personal data or restriction of processing or to object to processing, and (6) the right to lodge a complaint with a supervisory authority.

Boozt draws attention to the complainant's difficulties in interpreting the documents that have been shared. This has been corrected in conversations between Boozt Customer Service and the complainant. Boozt is actively working to improve the information provided in the context of a request for access in order to clarify the link between the data provided in raw data format and the related and explanatory documentation.

As regards the delay, the complainant received access to her data on 25 March 2020 and, according to Boozt employees, the delay was notified over the telephone in connection with the numerous calls made with Boozt Customer Service. However, Boozt has not confirmed in writing that Boozt was unable to provide the information within one month of the request, together with an explanation and information that the complainant may lodge a complaint with the supervisory authority, as Boozt would thus have done and in accordance with the provisions of Article 12(3) and (4) (when the complainant's request was received in electronic form and to demonstrate liability on the part of Boozt). Thus, only on 25 March 2020 and at the time of the submission of the information, the complainant receives a written statement as to why it took Boozt more than one month to comply with the request for access.

As regards the *completeness* of the data, the complainant's second request for erasure was dealt with on 11 February 2020. Therefore, the copy of data provided to the complainant in the context of the response to the access request of 25 March 2020 did not contain e-mails already deleted following the complainant's request for erasure. Information about these data must instead have accompanied the notification that the data have been deleted. All emails sent or received by Boozt from the complainant after 11 February 2020 should, according to Boozt routine and automated functions, have been provided to the complainant in the reply to the complainant's request for access. Boozt is happy to address and investigate to the extent possible specific questions as to which e-mails the complainant considers to be missing.

Some e-mail correspondence containing information needed in the ongoing handling of complaints and defence of legal claims has been excluded from automatic erasure on the basis of Boozt's legitimate interests. In so far as it contains information which could not be distinguished from information about Boozt, its employees or other data subjects, Boozt must have informed that those emails are not included in the copy provided to the complainant, together with a statement and information on the complainant's rights. Unfortunately, Boozt does not retain the notice and the explanation to be attached or provided when copies of the complainant's data were provided to the complainant on 25 March 2020.

Continued processing for accounting purposes

The complainant's personal data has continued to be processed for accounting purposes.

Boozt needs to keep certain personal data in order to fulfil its legal accounting obligations, such as supporting documents such as invoices and receipts describing and confirming business events. The data stored relates to goods, amount, VAT, payment method and if the customer used a gift card etc., order number, verification number, time, currency, country to which the sale was made, customer name, customer address and order history. In this context, "order history" refers to the goods purchased (the "cash sale"), any returns of goods already purchased (cash refund), and actual payouts (cash payment), linked to a customer identified by name and address.

The processing is based on a legal obligation (Article 6(1)(c)), namely Chapter 5, Section 7 of the Accounting Act (1999:1078) and Chapter 11, Section 8, point 5 of the VAT Act (1994:200). Therefore, there are obstacles to erasure pursuant to Article 17(3)(b) GDPR. The data will be processed for as long as necessary under this obligation, in the current circumstances and in relation to the complainant's personal data, for a further seven years from the respective business event.

Continued processing for handling of complaints

The complainant's personal data has continued to be processed for the purpose of handling complaints.

Below is the legitimate interest of the company in retaining data in order to demonstrate that it has fulfilled its commitment with regard to the complainant's five complaints. The processing is based on legitimate interest (Article 6(1)(f)) and obstacles to erasure exist under Article 17(1)(c) even after the complainant's objection (Article 21), since Boozt considered that there are legitimate grounds that outweigh the complainant's interests. This data is processed for a period of three years from the time of purchase.

Continued processing for the defence of legal claims

The complainant's personal data has continued to be processed for the defence of legal claims.

The processing is based on a legitimate interest (Article 6(1)(f)), since Boozt has a legitimate interest in defending legal claims in connection with the complainant's notification to the Danish consumer courts (Forbrugerombudsmanden, E-mærket and Center for Klageløsning), if and when necessary to process data within the communication made and any additional information relevant to the case. Similarly, data are also processed related to this supervisory matter, including data added through the annex to this supervision. Thus, there are obstacles to erasure under Article 17(3)(e). Data will be processed for as long as legitimate reasons remain in the light of the processes and timeframes of any appeal.

Continued processing for the prevention of misuse of services and fraud

The complainant's personal data has continued to be processed for the prevention of misuse of services and fraud.

Legal basis for processing

The processing is supported by a legitimate interest (Article 6(1)(f)) and there is an obstacle to erasure under Article 17(1)(c) even after the complainant's objection under Article 21, since Boozt considered that there are decisive legitimate grounds that outweigh the complainant's interests. Boozt has a legitimate interest in both being able to assess and react on an ongoing basis in the event of misuse of the company's terms and conditions of sale and delivery, including the company's Fair Use policy, which is at issue here and, on an ongoing basis, to be able to review and reassess its assessment of whether the complainant, through her purchasing behaviour, will continue to be blocked from purchasing additional goods from the company. The processing is done by analysing purchasing behaviour in relation to the company's terms and conditions of sale and delivery, which leads to an assessment of whether the complainant violated the company's Fair Use policy. The assessment is initially automated, but always only after a manual review. The continued processing, after established buying behaviour in violation of the company's Fair Use policy, takes place in order to be able to continuously re-evaluate the company's assessment, and to respond to legal attacks.

The data processed and the storage period

The data processed are, among other things, names and contact details. The data are processed for the purpose of maintaining the blocking of the complainant. The order and return history is processed in order to respond to questions and objections raised by the complainant regarding the assessment which led to the blocking of the complainant and to reassess that assessment at the request of the complainant. The information that, according to the Company's assessment, the complainant violated the Fair Use policy, as well as information to identify him when trying to make new purchases (by name, telephone number, email and address), is also necessary in order to block the complainant from further purchase for a period of time in accordance with this policy. No special categories of data or privacy-sensitive data are processed. In cases where the data reveals abnormal behaviour and in connection with certain misuses according to Fair Use, this has been considered and security measures have been put in place to restrict the processing organizationally and technically.

The data are processed for a period of three years from the last time the complainant was refused to make a purchase with Boozt on the basis of the Fair Use policy. As far as the complainant is concerned, Boozt states that: The complainant has requested the erasure of the data in the account. When the erasure — although partial — was carried out, the complainant was no longer able to log in to that account. This means that the retention period applicable to the complainant should be counted from the date of the last rejected order before the erasure was carried out.

What personal data need to be processed and how long they need to be processed for the purpose of maintaining or suspending a blocking in accordance with the company's Fair Use policy is set in relation to the customer's interests, fundamental rights and freedoms. This means a difficult balance, as more data often lead to more accurate and fair assessments, which both the company and its customers normally have an interest in, but at the same time lead to a greater interference with the rights and freedoms of data subjects. The Company processes the personal data that, after a balance of interests, has been deemed necessary to assess whether someone is abusing the Company's terms and conditions of sale and delivery, including the Fair Use Policy. If, on the basis of this information, a misuse is suspected, an individual assessment is made, in some cases, that the customer in question will be blocked from further purchase for a certain period. Since this is an intrusive decision, the

company cares that the information on which the decision is based is both accurate, relevant and available for subsequent assessment. This is in order, in the event that the data subject raises an objection, to make a new assessment, which may lead to the customer no longer being blocked from purchase. A new assessment is dependent on the fact that new information and the customer's arguments can be compared with the information on which the original decision was based.

No data other than the fact that the complainant is flagged as blocked under the Fair Use Policy is processed for this purpose other than the data already processed because of the company's accounting obligation.

Fulfilment of the conditions of the legal basis legitimate interest

Boozt notes that the complainant questions whether the complainant's *conduct constitutes an actual misuse* in accordance with its Fair Use policy. However, it is specifically to assess this that the company has the data and why they continue to be needed. The information is important for the assessment and according to the information provided regarding the Fair Use policy. The company considers that the byta's purchasing behaviour is contrary to the company's terms of sale and delivery and needs to be able to respond to this in other instances and to be able to evaluate its position on an ongoing basis.

It understands that the complainant also questions the legality of the Fair Use policy by claiming that it undermines and circumvents its statutory right of withdrawal of 14 days as a consumer. In this regard, the Company argues that the Fair Use Policy does not apply to orders already approved. It does not therefore prevent a customer from returning a product purchased from the company, but only in specific cases prevents a customer from making a new purchase from the company. The Company considers that the Fair Use policy does not violate the consumer's statutory right of withdrawal or any other consumer law regulation and that the processing of personal data within the framework of this purpose falls within the scope of "legislation".³ The purpose of the right of withdrawal is for the consumer to have the right to try and examine goods that the consumer has purchased. This is because the consumer cannot physically see the goods before the contract is concluded. However, the aim is not to allow consumers to borrow clothes free of charge and, for example, repeatedly buy the same product of the same size and return the same. Having a policy whereby a company chooses to inform that it will not enter into contracts with customers who through its repeated behaviour has shown that they do not have an intention to keep purchased goods is not contrary to consumer law. Like all companies, Boozt has contractual freedom and the right to enter into or deny new contracts. Since Boozt neither discriminates nor has a market dominant position, there are no obstacles to denying a purchase. On the other hand, the Fair Use policy never affects purchases already made. Boozt also offers free returns to its customers, and thus does not use its statutory option to charge for returns, and offers its customers a simple return procedure whereby Boozt perceives that it instead strengthens consumers' rights in this area. Finally, it should be pointed out that the cases brought by the complainant against the company at various instances in Denmark have not so far resulted in a decision or the like which led it to reconsider that assessment.

Through its balancing of interests, Boozt has identified and put in place the following *protective measures* to mitigate the risks that may arise from the processing:

³ As described in the Article 29 Working Party Opinion 6/2014 on the notion of legitimate interests of the controller in Article 7 of Directive 95/46/EC of 9 April 2014, WP 217, p. 26(f).

1. Access to patterns in a purchase behaviour identified and investigated for violations of Boozt Fair Use policy and details of the customers Boozt has chosen not to agree with for a period is strictly limited to the few employees who take and have the opportunity to reconsider decisions under the Fair Use Policy.
2. An analysis of previous buying behaviour in order to detect violations of the Fair Use policy takes place only when a customer has approved Boozt terms of purchase and then initiates an attempt at a new purchase. Information that Boozt has the ability to cancel an order is also provided when an item is placed in the shopping cart, as well as in connection with the completion of an order. Boozt strives to be as transparent as possible in its communication, through the Fair Use Policy and information in connection with purchases, with the factors taken into account when assessing whether someone violates the policy, while precise limit values or parameters cannot be given because there must always be an assessment in the individual case and because both fraud and misuse of Boozt business offer are not rarely organised and the same harm would soon occur with a different pattern and without detection.
3. Free returns and good terms and conditions of purchase are an important part of Boozt's offer and Boozt is careful to inform that a decision not to agree with a customer only takes place if a customer violates the Fair Use policy.
4. A customer who has been denied shopping is always asked to contact customer service and the Fair Use team if they have questions so that Boozt can explain and be given the chance to reconsider the decision. Boozt also takes, when deemed appropriate, the initiative to ask questions to avoid misunderstandings, if a buying behaviour that is not entirely obvious fraud, but harmful perhaps both to Boozt and the customer, is detected.
5. The analysis of buying behaviour does not capture individual behaviours, but only where there are repeated patterns (temporary deviations then have no or little impact).
6. Boozt investigates when there is room for alternative solutions and not to make a decision not to agree with a customer despite violations of the Fair Use policy, e.g. that someone in the Fair Use team contacts the person in question and sees if they want to provide an explanation.

The complainant also contends that the company does not restrict *access to the* data to the persons who need it for a specific purpose. The employee with whom the complainant was in contact, as is apparent from the complaint, and who, on 30 December 2019, explained the grounds for its blocking under its Fair Use policy, had access to the data as the policy manager.

As regards the complainant's *reasonable expectations*, Boozt, like other e-commerce operators, has always reserved the right not to purchase if there is reason to believe that the buyer intends to circumvent the contract or does not intend to keep the goods. The Fair Use Policy is both a clarification of the same terms and conditions previously applicable to purchases and a natural development in Boozt's interest in ensuring that both parties enter into the agreement with common interest. It may be considered common knowledge and industry practice that traders both process data about and analyse purchase patterns, for many purposes, including detecting behaviours covered by the Fair Use Policy.

In addition, the complainant was informed of the content of the Fair Use policy in its terms and conditions of sale and delivery at least 12 months before the decision not to enter into an agreement with it was taken. The complainant has been provided and

accepted the terms and conditions of sale and delivery of Boozt, including the above-mentioned information, each time the complainant has completed an order with Boozt during the 12-month period.

The policy stated the following during the relevant period.

»Infringement

If the Customer misuses obligations under these Terms of Sale and Delivery, Boozt.com may cancel or restrict the Customer's use of the Boozt.com website, which means that no orders can be placed. The following are considered to be, inter alia, a substantial infringement:

- *The customer provides incorrect information regarding name, address, email address, telephone number*
- *The customer harasses Boozt.com, our employees or our customers*
- *Boozt.com further reserves the right to cancel or limit the customer's future use of the Boozt.com website or charge the customer for any future return costs in the event that Boozt.com deems that the customer misused its account or returned products or exhibits a buying behaviour or an exercise of free return rights that causes or risks incurring Boozt.com's costs, risks or liability that go beyond normal use.*

When a question arises regarding the possible suspension, limitation or charging of return shipping costs, Boozt.com reserves in its application of the above provisions, the right to consider past events and the particular circumstances of the case. Boozt.com may choose to indulge in incidents and act as we deem most appropriate.'

To underline that it is not only "invalid data" and "harassments" that are considered unacceptable and may lead to blocking, the same conditions also state that other misuses, such as the misuse of discount codes, will "permanently block your ability to shop at Boozt.com":

In the event of fraud, attempted fraud or in the event of suspicion of other illegal activities in connection with the redemption of discount codes, we have the right to cancel the order using the discount code and we can permanently block your ability to shop at Boozt.com.

In addition, Boozt also refers to the privacy policy in force during the same period. The Privacy Policy clearly states that the personal data can also be processed for the purpose of assessing fraud and risks. Overall, it is clear that a customer who violates the terms and conditions risks being subject to limitations in the ability to place orders from Boozt.com.

Before informing the complainant of the decision not to enter into a contract due to the breach of Fair Use, Boozt considered other alternatives to blocking, such as temporarily preventing the complainant from acting and restricting the right to free return. In view of the extent of the complainant's conduct, it considered that the most appropriate solution was to prevent the complainant's future use of the platform. Other available options were not considered sufficient to put an end to the current behaviour. If the customer's conduct had consisted of an abnormal use of the right of withdrawal, the refusal to return free of charge would probably be an appropriate option, but in the present case the customer's behaviour consisted of an abnormally high frequency of quality claims for the products purchased. A customer who has a quality claim on the products is likely to make these claims regardless of whether the return is free of

charge or not. The mere refusal to return free of charge to the customer would likely have led to the continuation of the misuse of the services.

In addition, during the processing of this case, Boozt has reviewed and clarified its Fair Use policy.

Statement of reasons for the decision

The review in the case refers to the processing of the complainant's personal data based on the circumstances of the individual case and not whether the processing is lacking in general. In the decision, IMY has not taken a position on the possibility of processing personal data in general with reference to a Fair-Use policy.

Request for access

According to Article 15 of the GDPR, entitled 'Right of access by the data subject', the data subject shall have the right to obtain from the controller confirmation as to whether personal data concerning him or her are being processed and, where that is the case, access to the personal data and information referred to in paragraph 1.

Article 15(3) requires the controller to provide a copy of the personal data undergoing processing. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

The investigation shows that the complainant exercised her right of access under Article 15 on 30 January 2020 and that BOOZT replied to the request on 25 March 2020.

In order to comply with *the information requirements*, set out in Article 15(1)(a) to (h), Boozt provided the complainant with copies of its policy documents. IMY has no reason to question the completeness of the information provided in these documents in order to meet those requirements. However, the procedure does not meet the requirement of Article 12(1). According to that provision, the controller shall take appropriate measures to provide any communication under Article 15 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. IMY considers that the data subject cannot be expected to access such policy documents in full in order to understand what is relevant in his or her case. Since the information must be provided in writing, and it has not been established that the complainant has requested to receive information orally, this lack of information is not rectified by the fact that the company has completed the information orally. Boozt therefore infringed Article 12(1) and Article 15(1) in relation to the complainant's request for access.

At the same time, Boozt also provided the complainant with a *copy of the data* in order to comply with the requirement of Article 15(3). As regards the *completeness of the information*, there has been no evidence to support the complainant's claim that the information was incomplete and which would call into question the company's

statement that the copy contained all the information processed at the time.⁴ The investigation therefore does not show that BOOZT has infringed Article 15(3).

IMY does not consider that there is any reason to call into question the actual duration of the case given the circumstances of the case. On the other hand, when it comes to *informing about the delay*, IMY notes that it took about two months for the company to comply with the request. If the processing of the request takes longer than one month, the controller shall, in accordance with Article 12(3), before that inform about the delay and the reasons for it. Since the information must be provided in writing, and it has not been established that the complainant has requested to receive information orally, this lack of information is not rectified by the fact that the company has completed the information orally. IMY notes that the company within one month neither having complied with the complainant's request nor having informed the complainant in writing of the delay. Boozt therefore infringed Article 12(3) in relation to the request for access.

Request for erasure

According to Article 17(1)(a), the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed. Article 17(3) lists exceptions to this right.

The investigation shows that the complainant exercised her right to erasure under Article 17 on 28 November 2019. On 23 December 2019, the complainant received a notice from the company, which, according to the company's assessment, incorrectly gave the impression that the information underlying a blocking under the Fair Use policy should also be deleted.

IMY notes that if the controller does not act on the request of the data subject, the controller shall, pursuant to Article 12(4), inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy. From this also follows a requirement to inform about the continued processing, since the individual otherwise cannot decide whether to take legal action to safeguard his or her right.

Since Boozt did not inform about the further processing or the possibility of seeking a judicial remedy, it has infringed Article 12(4) concerning the request for erasure. The company's argument that it sought to correct the incorrect information in subsequent communications on 30 December 2019 does not change this assessment, especially not when it only contained information that the complainant had been blocked from further purchase and the reason for it, not about the continued processing.

In the following, IMY takes a position on the request for erasure of the data that the company has decided not to delete.

⁴ See prop. 2017/18:105 p. 107 et seq., judgment of the Court of Justice of the European Union of 17 July 2014 in cases C-141/12 and C-372/12 and the Administrative Court of Appeal in Gothenburg judgment of 17 September 2019, Case No 1677-19.

Continued processing on the basis of a legal obligation

According to Article 6(1)(c), processing is lawful if it is necessary for compliance with a legal obligation to which the controller is subject. Pursuant to Article 17(1)(a), the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed. Under Article 17(3)(b), the data subject does not have the right to have his or her data erased pursuant to Article 17(1) to the extent that processing is necessary for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject.

Accounting purposes

IMY takes the view that there has been no reason to call into question the legality or necessity of the company's processing of the complainant's personal data for *accounting purposes* according to Article 6(1)(c).

Communication logs

IMY takes the view that there has been no reason to call into question the lawfulness or necessity of the company's processing of the complainant's personal data in the communication logs maintained by the company in order to demonstrate compliance with its obligations under i.a. the GDPR and as part of accountability under Article 5(2) and Article 24 pursuant to Article 6(1)(c).

Continued processing on the basis of legitimate interests

Applicable provisions, etc.

For processing to be able to rely on Article 6(1)(f) of the GDPR, all three conditions laid down therein are met, namely (1) that the controller or a third party have a legitimate interest (*legitimate interest*), (2) that the processing is necessary for the purposes of the legitimate interest (*necessary*) and (3) that such interests are not overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data (*balance of interests*).

Recital 47 of the GDPR states i.a. the following. The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or 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 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 personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interests of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

In IMY's view, the 'legitimate interest' condition should not be interpreted restrictively. The decisive factor should be whether the interest is permitted by law or is otherwise generally recognized in a society based on the rule of law. For example, a purely economic interest in merely creating or maximising economic profit may be such an interest, although such an interest may weigh relatively lightly in the balancing of interests.⁵ However, an interest cannot be justified if it is contrary to legislation, e.g. if a competent authority or court has determined that a particular interest is illegal, e.g. contrary to good marketing practice according to the Marketing Act.

It follows from the case-law of the Court of Justice, with regard to the condition 'necessary', that exceptions and limitations on the protection of personal data must be limited to what is strictly necessary.⁶ That condition must be examined in conjunction with the principle of data minimisation laid down in Article 5(1)(c). The examination to be carried out involves verifying that the legitimate interest which the processing is intended to protect cannot reasonably be protected in an equally effective manner by other means which less prejudice the fundamental rights and freedoms of data subjects, in particular the right to respect for private life and the right to the protection of personal data as enshrined in Articles 7 and 8 of the Charter.

As regards the third condition, *balancing* of interests, the seriousness of the violation of the rights and freedoms of the data subject is a central element. Account must be taken i.a. of the nature of the personal data in question, in particular if they are sensitive data. In addition, account must be taken of the nature of the processing and how it is carried out, taking into account in particular the number of persons who have access to the personal data and the means of accessing them. The data subject's reasonable expectation that his or her personal data will not be processed is also relevant if, in the circumstances of the case, the data subject cannot reasonably expect such processing to take place.⁷

According to Article 4(4) of the GDPR, profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

General about the assessment

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

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

⁵ See e.g. Supreme Court of Norway (Høyesterett) judgment of 7 December 2021-12-07 (HR-2021-2403-A, case No 21-055809SIV-HRET), paragraph 66, available here <https://www.domstol.no/globalassets/upload/hret/avgjorelser/2021/desember-2021/hr-2021-2403-a.pdf>.

⁶ Judgment of the Court of Justice of the European Union Rīgas satiksme, C-13/16, EU:2017:336, paragraph 30 and the case-law cited.

⁷ Judgment of the Court of Justice of the European Union TK, C-708/18, EU:2019:1064, paragraphs 47-48 and 56-58. The CJEU has confirmed that this case-law applies to the GDPR, see judgment in M.I.C.M., C-597/19, EU:2021:492, paragraph 107.

IMY proceeds to examine whether the company has been able to demonstrate a legal basis for continuing the processing of complainant's personal data for the respective purposes.

Objection to the processing for handling complaints

The complainant has objected to the processing of the complainant's personal data which the company has stated that it carries out on the basis of the legitimate interest of demonstrating that the company has fulfilled its commitment with regard to five complaints of the complainant's.

IMY considers that the interest indicated by the company is legitimate. Furthermore, the processing appears to be strictly necessary for the purpose. The data is also not too extensive or privacy sensitive.

In the balancing exercise between the legitimate interest of the company and the interests, rights and freedoms of the complainant, IMY considers that *the company's legitimate interest* weighs heavily. Furthermore, the processing appears to be something that the complainant can reasonably expect when complained about a purchase. The processing does not appear to be an infringement of privacy and the data itself is not privacy sensitive. In an overall assessment IMY considers that the *complainant's interest* in not having her data processed does not outweigh the company's legitimate interest.

In those circumstances, the company was entitled to continuing the processing of the data and was not at the time obliged to erase them.

Objection to the processing for defence of legal claims

Under Article 21(1), the complainant has objected to the processing of the complainant's personal data, which the company has stated that it carries out on the basis of the legitimate interest of defending legal claims in connection with the complainant's complaints to Danish consumer bodies (Forbrugerombudsmanden, E-mærket and Center for Klageløsning). In addition, data is also processed if and when it's needed within the communication carried out, as well as any additional information deemed to be relevant in the cases.

In the *balancing* between the legitimate interest of the company and the interests, rights and freedoms of the complainant, IMY considers that the company's *legitimate interest* weighs heavily. Furthermore, the processing appears to be something that the complainant can reasonably expect when commenced proceedings before consumer bodies. The processing does not appear to be an infringement of privacy and the data itself is not sensitive. In an overall assessment IMY considers that the *complainant's interests* in not having her data processed does not outweigh the company's legitimate interest. In those circumstances, the company was entitled to continuing the processing of the data and was not at the time obliged to erase them.

Objection to the processing for prevention of misuse of services and fraud

Boozt has, after the complainant's request for erasure, continuing the processing of the complainant's personal data which the company has stated that it carries out on the basis of the *legitimate interest* of being able, on an ongoing basis, to be able to assess and react in case of misuse of terms of sale and delivery, including the company's Fair Use policy, and, secondly, to review and reassess the company's assessment, where appropriate, whether the person blocked (i.e the complainant)

through her purchasing behaviour should continue to be blocked from further purchases of goods from the company.

Has the company demonstrated that the interest is legitimate?

IMY notes that recital 47 of the GDPR states that processing of personal data strictly necessary for the purposes of prevention fraud constitutes a *legitimate interest* of the data controller concerned.

The Article 29 Working Party⁸ has previously stated that prevention of misuse of services can be considered as legitimate 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.⁹ In that context, it should be pointed out that the concept of ‘misuse of services’ in that statement appears in an exemplification of criminal conduct, and that it has not in any way been shown that the misuse of terms of sale and delivery attributed to the complainant is criminal. In this context, however, it should be pointed out that if the company through the proceedings would process personal data of the complainant relating to criminal offences within the meaning of Article 10 of the GDPR, in addition to the legal basis in Article 6, the company would also need legal support for the processing for the purpose in question in Article 10.¹⁰

In the present case, it has not been established that the interests relied on by the company that the processing is intended to protect, including its Fair Use policy, or the procedure entailed by that policy, is in conflict with any relevant legislation, such as consumer law.

Against this background, IMY considers that the company has a legitimate interest of preventing misuse of its terms of sale and delivery, including its Fair Use policy, and continuously being able to reassess the blockage.

Has the company demonstrated that the processing is necessary?

IMY considers that the processing is *necessary* for purposes relating to the legitimate interest. The investigation shows that the data are relevant for both maintaining the blocking and continuously reevaluate it. The interests which the processing is intended to protect cannot reasonably be protected in an equally effective manner by other means which less prejudice the complainant’s right to respect for private life and to the protection of personal data as enshrined in Articles 7 and 8 of the EU Charter of Rights. For example, to completely stop offering free returns to all customers does not appear to be a reasonable means.

Has the company demonstrated that the processing is permitted based on a balancing of interests?

In the context of the *balancing* of interests between on the one hand the legitimate interests of the company and on the other hand the interests, rights and freedoms of the complainant, IMY notes the following.

IMY finds that the company’s legitimate interest weighs relatively heavily and appears — anything else similar — to be more considerable than the complainant’s interest in

⁸ 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, the Working Party has been replaced by the European Data Protection Board (EDPB) (see Articles 68 and 94(2) GDPR).

⁹ Article 29 Working Party Opinion 6/2014 on the notion of legitimate interests of the controller under Article 7 of Directive 95/46/EC adopted on 9 April 2014, [WP 217](#), p. 25.

¹⁰ See IMY, Legal Position IMYRS 2021:1 — the meaning of the term “personal data relating to criminal offences” in Article 10 of the GDPR of 8 December 2021.

not having her personal data processed and the possibility of entering into new agreements with the company during the current blocking.

In assessing the *seriousness of the infringement of the complainant's rights and freedoms*, IMY notes the following. *The consequences* for the complainant consist of the refusal, for a certain period of time, to make further purchases from the company, which is one of several actors offering similar purchasing opportunities on the market. In terms of the *type of data* it is not in itself question of privacy-sensitive or sensitive data. *The type of processing* consists of an automated analysis of the complainant's buying behaviour over time involving profiling, which is to be regarded as a privacy-sensitive processing, which may entail risks, in particular in automated decision-making. Regarding the *origin and dissemination* of the data, they were obtained directly from the complainant in her interactions with the company and are not disclosed to third parties. Those who have access to the data are a limited group of persons and they only have access to the data when they need it as part of their duties to apply the policy, such as the employee with whom the complainant was in contact. Overall, IMY considers that this means that the processing constitutes a violation of the complainant's fundamental rights and freedoms of a certain degree of seriousness.

In the balancing exercise, particular attention must be paid to the complainant's *reasonable expectations* and, in that regard, to the relationship between the company and the complainant, for example if the complainant is a customer of the company. It also follows from the expression 'reasonably' that the assessment refers to what an average member of the collective of data subjects can be assumed to expect. Particular attention should be paid to the way in which the company has informed the complainant of the processing, in particular if the company has informed the complainant in such a transparent manner that goes beyond the obligations laid down in Article 13, in so far as such information is also provided *before* the processing is actually carried out.

In assessing what the complainant could reasonably expect in the present case, the processing appears to be something that an average customer, i.e. a repeat customer buying and returning goods free of charge, could possibly expect, but far from self-evident. In IMY's view, the information provided by the company in its wording at the material time was also not clear in a way that could be balanced for that purpose. In IMY's view, that information appears rather difficult to access and appears to target other infringements and measures, which is to some extent supported by the fact that, during the period of that supervision, the company found reason to revise and clarify the policy. Since such clarification cannot, in any event, heal a lack of information that should have been provided before the commencement of processing, there is no reason for IMY to decide whether the company's current policy is sufficiently clear. The fact that the company referred to the policy — before the complainant made her first purchase and at each subsequent purchase — and, finally, when the actual blocking decision was taken and implemented, is irrelevant in that context. In those circumstances, IMY considers that the complainant could not reasonably have expected the processing of personal data.

Finally, the balance must consider *the protective measures taken to mitigate the risks associated with the processing*. In doing so, the company has put in place a number of safeguards to reduce the risks that may arise from the processing. The risks of automatic profiling have been reduced by the fact that the blocking decision was preceded by an individual and manual examination, that the complainant was informed of the blocking and the reasons for it, and that the company had in place procedures

and a procedure for reviewing the decision at the complainant's request. All of these measures, according to IMY's assessment, speak with some strength in favour of the company in the balancing exercise. To a certain extent, the fact that it has not emerged in the case that the company has sufficiently examined alternative solutions in relation to the complainant, such as no longer offering the complainant free returns instead of a complete blocking, speaks to the company's disadvantage. The fact that the complainant, according to the company, has high quality claims cannot in itself neither lead to the conclusion that she did not intend to retain purchased goods, nor that charging of future return costs would not be an appropriate first alternative in relation to the complainant.

When *assessing the* above factors, IMY finds Boozt has not been able to support the current processing of the complainant's personal data on a balancing of interests according to Article 6 (1) (f) of the GDPR. No other legal basis has been relevant to apply to the current processing.

By the fact that Boozt, at the time of the request for erasure on the 28 November 2019, having continued to process the complainant's personal data for the purpose of prevention of misuse of services and fraud without being able to demonstrate a legal basis for the processing, the company has processed the complainant's personal data in breach of Article 6 (1) of the GDPR.

Choice of corrective measures

IMY has found that the company has failed to deal with the complainant's request for access and erasure and processed the complainant's personal data without legal basis as set out above. It follows from Article 58(2)(i) 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) determines the factors to be taken into account when imposing administrative fines and determining the amount of the fine. In the case of a minor infringement, IMY may, as stated in recital 148, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Account needs to be taken to aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement as well as past infringements of relevance.

IMY notes the following relevant facts. The violations have affected one person. It has not applied to sensitive data and the company has not previously received any corrective action for breach of data protection regulations. Furthermore, Boozt has done its best to remedy the shortcomings arising from its incorrect handling of the complainant's requests and worked to improve its procedures and information to data subjects. Against this background, IMY considers that it is such minor infringements within the meaning of recital 148 and that the company must be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

Further, IMY finds reason to order Boozt pursuant to Article 58(2)(d) of the GDPR to ensure that the complainant's personal data the company collected and processed at the time of the request for erasure on the 28 November 2019 for the purpose of preventing misuse of services and fraud are no longer processed for that purpose, and to inform the complainant of those measures in accordance with Article 12(3). The measures shall be implemented no later than two weeks after this decision becomes legally binding.

This decision was taken by the Head of Unit [REDACTED] following a presentation by the legal advisor [REDACTED].

Annex

Complainant's identification data

How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection (IMY). Please indicate in your letter the decision you want to appeal and the amendment that you are requesting. The appeal must reach the Swedish Authority for Privacy Protection no later than three weeks from the date on which you received the decision. If the appeal has been received in due time, the Swedish Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can send the appeal by e-mail to the Swedish Authority for Privacy Protection if the appeal does not contain any sensitive personal data or information that may be subject to confidentiality. The Swedish Authority for Privacy Protection's contact details are set out in the first page of the decision.