REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

FINAL ADOPTED DECISION
(IMI case nr 441345)

26.01.2023

Notice of termination of the proceedings concerning the protection of personal data

Estonian Data Protection Inspectorate (SA Estonia) received a complaint through IMI system (case nr 441345) from SA Spain. Since the controller [redacted] has its main establishment in Tallinn, Estonia, Estonian DPI accepted the case as LSA.

The complainant ([redacted]) is a Spanish resident. The complaint was the following: *He made two purchases on consecutive days of the same product (a software licence) on the* [redacted] *website. When he made the second purchase, the transaction was blocked and he was requested to take a selfie in which he had to appear holding his ID card, to verify that he was the one making the purchase. He addressed the AEPD requesting help. The legitimacy of the data processing (selfie with the ID) in relation to the purpose pursued is not sufficiently justified. Excessive processing of personal data may take place.*

SA Estonia contacted the Controller and asked for explanations regarding their processes of collecting customer´s photos with ID cards. The questions and replies below:

1. **When does** [redacted] **recquire ID card based customer´s verification?**
   ID card based verification takes place in order to avoid internet-based fraud which is very common. The need to verify a person comes from a warning signal given by the fraud prevention system. This system rates the customer from 0-100 points. The rating criteria includes customer´s device, payment method (or payment methods, in case there are more than one), customer´s user accounts (in case there are more than one) etc. If the user rating based on the previous criteria is from 60-100 points, the transaction or customer status changes to high risk level. In order to avoid a crime being committed, the Controller must verify that the customer is the owner of the Credit card.

2. **Does the controller´s Privacy Policy include the conditions of when ID card based verification is requested and is it visible on controller´s website?**
   Our Privacy policy states that : *The personal data we collect about you will depend on the activities that have been performed through our website. Typical types of personal information include: ID and contact data include your name, address, email address, date of birth and any personal information provided in communications with us.*[1]

[1] [redacted]

We do not collect personal data (like ID verification) unless there is a warning signal that a fraud could be committed. As our Privacy Policy states, we do not keep the data longer than is needed to finish the process. In similar cases we compare the Payment method owner with the verified person and all ID-based data will be deleted after that.

3. **What kind of signals did you receive about the Complainant that suggested a suspicious activity might take place? Why did you have to ask for his photo with ID card?**

[redacted] registered his account on our website on 2017 and bought a few items without an additional verification. On 2021 he tried to create a new account with a different e-mail address and using [redacted] payment method but the e-mail that was attached to [redacted] was the same as on the first account that was created in 2017. Taking into consideration that the new account was not verified but the payment method used was the same [redacted] account that was attached to the first account, our system registered this as a high risk activity. When the customer tried to make a purchase and the system gave a signal that the owner of the payment method must be verified, the transaction was blocked and the customer was sent a notification. Since this incident signalled that an illegal payment method could be used, we did not have any other option but to verify the person by asking for a selfie with ID card. Customer´s Credit card was not blocked or credited and since the customer did not provide the necessary data, the transaction was cancelled.

Our Terms of Services state under Section 6 that a customer can have only one account: *You agree to create and use only one account on this website.* It also states that the *customer agrees to provide current, complete and accurate purchase and account information for all purchases and agrees to promptly update your account and other information, including e-mail address and Credit card numbers and expiration dates.*[2]

During the investigation SA Estonia has proposed that [redacted] complements their Privacy Policy with the information regarding their collection of customer´s photo with ID card and the purpose of this collection.
The Controller has added information to their Privacy Policy: *Proof of Identity (Including a Photo ID with selfie)* and its collection purpose is: *To administer and protect our business, products, services, networks, systems, the website and data and property hosted on or made available through the website including implementing and monitoring security measures, troubleshooting, data and usage analysis, testing, system maintenance, support, reporting and hosting of data.*

The Complainant was asked for a selfie with his ID card due to security reasons and the Controller has explained its processes and reasons for doing so. Since this type of verification (selfie with ID card) is commonly used, it is performed only when customer´s activity is suspicious and proves to be against company´s Terms and Conditions (e.g creating several accounts with the same payment method), SA Estonia does not find it to be excessive processing of personal data. The Controller has declared that the photo/ID will only be used for verification purposes and will be deleted immediately after this process is finished so no storage of excessive data takes place.

To conclude, SA Estonia has asked the Controller to update their Privacy Policy in different languages and will terminate the proceedings regarding [redacted]

[redacted]

Best regards,

[redacted]
Lawyer
Authorized by Director General