FINAL DECISION

Datu valsts inspekcija

Blaumaņa iela 11/13-15, Rīga, LV-1011, tālr. 67223131, fakss 67223556, e-pasts info@dvi.gov.lv, www.dvi.gov.lv

[redacted]

Decision

in Riga
December 3, 2019 No. 2-2.2/52

Re: imposing an obligation

Data State Inspectorate of the Republic of Latvia (hereinafter - the Inspectorate) carried out an inspection of data processing by SIA [redacted] No.[redacted] (hereinafter SIA) based on a complaint from applicant [redacted] (hereinafter the Applicant), dated 21 January 2019 (hereinafter - the Complaint) transmitted by the Republic of Ireland and the consistency mechanism set out in Article 63 of the General Data Protection Regulation[1] (hereinafter - the GDPR).

The Inspectorate finds that the Complaint and the information in the attachment shows that on January 20, 2019 the Applicant contacted SIA by e-mail. The Applicant informed SIA about the erroneous registration on the SIAs website [redacted] and requested the removal of two registered profiles named [redacted] and [redacted] of Applicant. The Inspectorate finds that SIA, by e-mail dated January 21, 2019, provided the Applicant with a reply informing the Applicant that SIA could not comply with the Applicant's erasure request.

As part of the inspection, the Inspectorate requested and received information on 6 June 2019 from SIA (registered with the Inspectorate under No. 2-4.3/914-S). The Inspectorate notes that SIA, in its response letter dated June 4, 2019 (the Response Letter), inter alia, stated that *"We have blacklisted the email address* [redacted]*, so no e-mail will be sent to us "*.

Within its competence, the Inspectorate shall determine and indicate the following in the assessment of the above case.

According to Article 1 (2) of the GDPR, This Regulation protects fundamental rights and freedoms of natural persons and in particular - their right to the protection of personal data.

Article 2 (1) determines that This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

According to Article 4 (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'), however according to Article 4 (2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. It follows that an e-mail address, if it contains a person's name and surname, is to be considered as personal data and any processing of such data, including their blacklisting, constitutes processing of personal data within the meaning of the GDPR.

Pursuant to Article 4 (7) of the GDPR, the controller is responsible for the compliance of the processing of personal data with the Regulation, namely a natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of processing. In this case, SIA is responsible for personal data processing of the Applicant.

The Inspectorate indicates that processing of personal data must be carried out in accordance with the GDPR, including Article 6, which provides that the processing of personal data shall be lawful only if and to the extent that at least one of the legal grounds referred to in Article 6 (1) applies, namely, consent, performance of contract, legal obligation, public interest, protection of vital interests and respect for legitimate interests. In addition to providing the legal basis, the controller must also comply with other conditions laid down in the GDPR, such as Article 5 (1) (a) of the GDPR stipulating that the processing shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. However, Article 5 (1) (b) of the GDPR states that data shall be collected for specified, explicit and legitimate purposes. If these conditions are not met, the processing of personal data shall be incompatible with the GDPR and shall not happen.

Furthermore, in accordance with the principle of accountability set out in Article 5 (2) of the GDPR, it is the controller who has the responsibility to ensure that the personal data processing process which shows that the processing of personal data complies with data protection regulatory framework requirements.

In addition, pursuant to Article 24 (1) and (2) of the GDPR, the controller shall take appropriate technical and organizational measures to take account of the nature, extent, context and purposes of the processing and the various degrees of probability and severity of the rights and freedoms of natural persons. ensure and be able to demonstrate that the processing is in accordance with the GDPR. Thus, it is understandable that the controller provides the technical and organizational means to secure data processing.

Article 25 (1) of the GDPR determines that taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

Thus, it is understandable that the Controller provides the technical and organizational means to secure data processing.

Article 15 – Article of the GDPR 22 sets out the data subject's rights, which states that the data subject is entitled to request in writing the information set out in this Article related to the data subject's personal data.

Article 17 of the GDPR provides that the data subject has the right to request the erasure of his or her personal data. Article 17(1) and (2) of the GDPR lays down the right to “be forgotten”. In accordance with Article 17(1) of the GDPR, data subject has the right to obtain that the controller delete the personal data of data subject without undue delay, and the controller is obliged to delete personal data without undue delay if one of the conditions referred to in paragraphs 1 and 2 of this Article exists. It follows that the controller is obliged to respond to the data subject's request and delete the personal data of the data subject if any of the conditions set out in Article 17 (1) and (17) of the GDPR are met.

The Inspectorate evaluation of the complaint the information relating to the Applicant's personal data, concludes the following. Conditions of Article 17 (1) of the Regulation have been met and the data subject (Applicant) has withdrawn his consent to the processing of personal data on the basis, of which the SIA processed the personal data of the Applicant.

The Inspectorate, having assessed the information contained in the Response Letter to SIA, concludes that SIA is still processing the Applicant's personal data because the LLC has blacklisted the Applicant's personal data (email address [redacted]).

Having assessed the response provided by SIA, the Inspectorate concludes that there is no legal basis for SIA to continue processing and storing the Applicant's personal data (e-mail address [redacted]) in the SIA blacklist.

Article 31 of the GDPR states that the controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

Article 58 (2) of the GDPR provides that the Inspectorate, as each supervisory authority for the processing of personal data, has several corrective powers. Article 58 (2) (g) of the GDPR states that the Inspectorate shall have the power to order the rectification or erasure of personal data or to restriction of processing pursuant to Articles 16, 17 and 18 and to inform the recipients the data have been disclosed pursuant to Articles 17 (2) and 19.

Article 66 (1) of Administrative Procedure Law determines that in considering the usefulness of the issue of, or of the content of an administrative act (Section 65), an institution shall take a decision regarding: 1) the necessity of the administrative act for the attaining of a legal (legitimate) goal; 2) the suitability of the administrative act for the attaining of the relevant goal; 3) the need for the administrative act, that is, whether it is possible to attain such goal by means which are less restrictive of the rights and legal interests of participants in the administrative proceeding; and 4) the conformity of the administrative act, comparing the infringement of the rights of a private person and the benefits for the public interest, as well as taking into account that substantial restriction of the rights of a private person may only be justified by a significant benefit to the public.

Having assessed the information provided in this administrative act, the Inspectorate concludes that the detected infringement in the field of data protection of natural persons is continued, therefore, only the issuance of an administrative act can increase the SIA's awareness of its noncompliance with the GDPR and prevent repeated infringements. The administrative act is issued for the purpose of protecting the Applicant's rights to the protection of his personal data established in the Satversme (the Constitution). The Inspectorate finds that the relevant objective of this Decision cannot be achieved by less restrictive means of the SIA. There is no legal basis for SIA to process the Applicant's email address on the blacklist of SIA.

By this administrative act, the rights of the SIA as a private person are minimally infringed, while it is in the public interest to obtain assurance on the effective protection of personal data by the Inspectorate. In this administrative act, an infringement of the rights of the company as a private rightholder is proportional to the benefit of the public interest, the latter exceeding the first.

In view of the above and on the basis of Article 58 (2) (g) of the GDPR, Article 23 of the Personal Data Processing Act (hereinafter - FPDAL), Article 63 (1)(2) of the Administrative Procedure Law (hereinafter – APL), ***the Inspectorate shall decide:***

1. ***Impose an obligation to the SIA to delete the Applicant's personal data immediately, but not later than 20 December 2019 - the e-mail address [redacted] from the blacklist of SIA, as well as other possible storage sites, if data processing is carried out wholly or partly by automated means, or the Applicant's personal data are processed in a filing system or are intended to form part of a filing system where the processing is not carried out by automated means.***
2. ***The future activities of SIA shall comply with the requirements of the GDPR and other laws and regulations referred to in this Decision. SIA shall assess the different degrees of likelihood and severity of risks to the rights and freedoms of natural persons, taking into account the nature, extent, context, purposes and technical and organizational measures taken to protect personal data and prevent their possible unlawful processing. SIA shall provide a mechanism to prevent such situations from occurring in the future of SIA and prevent any inconsistencies, if any, by ensuring the legal processing and protection of personal data.***

Please inform the Inspectorate in writing of the execution of the order by **20 December 2019** *(last day for submitting a written reply to the mail or for sending electronically with a secure electronic signature).*

This decision is an administrative act within the meaning of the APL and will be notified to the SIA by post as a recorded mailing. Article 70 (1) of the APL determines that, provided that it is not otherwise stipulated in an external regulatory enactment or the administrative act itself, an administrative act shall come into effect at the time the addressee is notified of it. In accordance with Article 70 (2) of the APL and Article 8 (3) of the Law on Notification, A document which has been notified as a registered postal item shall be deemed notified on the seventh day after handing it over to the post office.

In accordance with Article 24(2) of the FPDAL, Article 70, Article 76(2) and Article 79(1) of the APL, this decision may be appealed to a court in accordance with the requirements laid down in Article 188 (2) and Article 189(1), Article 29(3) of the Law On Judicial Power and according to Decision No 307 of the Board of Justice of 5 March 2018 on Courts, Territories and Locations of their Activities - within one month from the date of their entry into force at the relevant courthouse of the Administrative District Court, at the location of the registered office of the Company.

Acting Director /signature/ [redacted]

[redacted]