TIETOSUOJAVALTUUTETUN TOIMISTO

Notice: This document is an unofficial translation of the Data Protection Ombudsman's final decision (national record no. 2206/171/20, IMI case register no. 177676). Only the Finnish version of the decision is deemed authentic.

Record no. 2206/171/20

16 February 2023

Decision of the Data Protection Ombudsman

The matter Data breach and data minimisation

Data controller Accommodation service provider [redacted]

Background to the matter

A data breach on the controller's computer system took place on Friday 13 March 2020. The controller's extranet service (customer self-service portal) was attacked and the ERP system it utilised as its interface. The attack was detected on 13 March 2020, while it was still ongoing, from abnormal log data behaviour.

The staff of the controller identified the vulnerability that had been used and corrected it immediately after its detection. This stopped the attack and blocked the attacker's access to the systems. Based on the log data, it can be verified that the attack had begun approximately 12 hours before the vulnerability was corrected. The log data and the investigation suggest that this was an automated search for vulnerabilities and automated testing of different types of SQL injections. The most part of them did not grant the attacker access to the system, but the attacker managed to utilise a vulnerability in the interface with one of them.

The first phase of the investigation took place the same day and, based on the methods detected and other discoveries, the preliminary estimate was that the attacker had not managed to access the data in the database (including personal data) through the interface vulnerability. The investigation continued Monday, 16 March 2020, and it was discovered that the attacker had gained access to the database.

Even though the vulnerability in the system was corrected, the attacker had managed to obtain personal data and it remains unknown what the attacker has done with this data. The cyber-attack gave the attacker access to approximately 165,000 personal data records, most of which were overlapping and contained data on the same data subjects.

14 complaints pertaining to the attack were submitted to the Data Protection Ombudsman's Office. The complainants are not parties of the case in the manner laid down in Section 11 of the Administrative Procedure Act (434/2003) as they do not have a right, interest or obligation affected by the matter. [1]

Information provided by the controller

By letter dated 3 July 2020, the Office of the Data Protection Ombudsman asked for clarification of the cyber attack against [redacted] system and the related breach notification. The

[1] 2338/163/20, 2372/163/20, 2401/163/20, 2402/163/20, 2411/171/20, 2492/182/20, 2648/163/20, 2776/171/20, 3051/154/20, 3187/163/20, 3292/153/20, 3636/154/20, 4871/153/20 and 6457/182/20

controller submitted the report on 14 August 2020 and replied to questions from the Office of the Data Protection Ombudsman as follows:

1. What personal data does [redacted] collect about its customers?

[redacted] is a provider of accommodation services and is the leading provider of furnished apartments in the Nordic countries. [redacted] focuses on providing services to corporate customers, but there are also private customers. The personal data collected depends on the category of data subjects that belong to and what data are necessary for the purposes of processing. Forenom has, for example, the personal data of tenants, business contacts and landlords.

Accommodation/Leases: service delivery and invoicing: contact information, date of birth, language, registration data (user ID and any other unique identifiers collected during registration), credit rating information (invoicing), camera surveillance, log data, code lock usage logs, call recording, instant messaging history.

[redacted] online store: contact information (address, phone number, e-mail), registration information (user ID and other unique identifiers collected during registration), purchase/behavior history data.

Customer service and communication: contact information, customer relationship information (information about newsletter subscriptions or customer contact requests).

Analysis, statistics and development of business, products and services: information on purchasing behaviour, customer feedback information.

Direct marketing and marketing campaigns: contact information (address, e-mail address and phone number), information about the newsletter subscription, purchase history data (targeting of marketing messages).

Analysis of the use of the website: information collected by cookies.

Access management: information on the status of the apartment (booked, free) and the availability of keys when guests leave and arrive.

2. On what basis does [redacted] process the personal data?

The table below specifies the legal grounds used by [redacted] for each of the purposes for which personal data are processed. The same set of processing may contain several different legal grounds on which the processing is carried out, but we have added a description of the situations to which each legal basis applies.

Purpose of processing and legal basis:

Accommodation/rental agreements, service delivery and billing

— Contract (contracts, supply of services)

— Consent (credit rating information)

— Legitimate interest (customer relationship management, customer service, detection of abuses and faults, camera surveillance, log data, code lock usage log data)

Forenom online shop

— The agreement

Customer service and communication

— Legitimate interest

Analysis, statistics and development of business, products and services

— Legitimate interest

Direct marketing and marketing campaigns

— Legitimate interest (business customers)

— Consent (private customers, newsletter subscription)

Analysis of website usage

— Consent

Access management

— Legitimate interest

3a. What is the storage period of personal data of the customers?

As a part of its GDPR project that was carried out before the Regulation entered into force, [redacted] established and collected the customer data it had collected to that date and documented or determined the storage periods of personal data where this had not been done.

The storage periods of personal data on customers are defined as follows:

Lessor and tenant information: 10 years from the expiry of the rental contact or other type of contract CRM data: 5 years from the most recent activity Invoicing information: as laid down in the accounting legislation (last 6 years + current year)

On account of the data breach of March 2020 and the following enquiries by customers concerning the data storage periods, [redacted] has re-examined the completed data inventory and the related personal data storage periods during the spring and summer and is currently considering whether a need to change the storage periods exist, and if this can be done without risking [redacted] business operations or statutory obligations.

3b. What will be done with the data after the end of the retention period?

At the end of the retention period specified by [redacted] or by law, the customer data will either be deleted or anonymised.

4a. Can customers delete their data from the Forenom customer records?

[redacted] customers can delete their [redacted] account (the web shop user ID) by logging into the account. [redacted] has appointed people responsible for processing other deletion request and developed an internal process for handling the deletion requests for personal data of data subjects. [redacted] is bound by legal obligations to retain certain types of personal data (for example, information on traveller notifications), but the personal data that is not in the scope of

statutory obligations can be deleted from [redacted] customer records upon a data subject's request within one month of receiving the request for deletion.

4b. If not, why not?

As a controller, [redacted] has statutory and commercial obligations to store some personal data of its customers. If the customers were given the chance to freely delete data, this would risk the realisation of [redacted] obligation to store data. [redacted] has assessed the alternatives and has concluded that the customers have the right to control their web shop accounts freely, but they have to request for the deletion of data pertaining to accommodation and rental activities and contracts in line with [redacted] protocol for the realisation of data subjects' rights, so that [redacted] as the controller can assess, in a case-to-case basis, which data can be deleted.

5a. How the personal data collected is protected (a) when the data is collected

Data is transferred via a secure HTTP connection from the user to our servers.

5b. How is the collected personal data protected (b) during storage?

The data is stored in encrypted databases and log files, accessed by a limited number of persons.

6. Other relevant issues?

Due to the updating of the data inventory, [redacted] privacy policy is also to be updated and internally approved, and the updated version has not yet been published. The updated privacy statement is attached to the reply to this request for information.

7. What measures have been taken or will be taken in relation to the data breach?

[redacted] has introduced an additional firewall layer to protect against attacks, restricted access to certain geographical locations, conducted a security audit for the source code of the system, and also introduced encryption for less relevant data.

As an organisation, [redacted] is committed to regular third-party security audits on [redacted] systems.

All staff participate in mandatory online training on the processing of personal data and data security. For those roles and teams that need deeper skills (e.g. sales, customer service and technology team), separate training materials will be introduced.

Hearing of the controller

By a hearing request sent on 16 April 2021, the controller was given the opportunity to comment on the preliminary assessment of the matter and on the facts set out in the request for a hearing. In addition, the Office of the Data Protection Ombudsman has reserved an opportunity for the controller to be heard on any corrective measure to be imposed in the case. In its reply of 18 May 2021, the controller stated, inter alia:

[--]

It could be verified that a part of the queries submitted by the attacker to the database have returned data from the database on the categories of data subjects as indicated below:

- *Customer data, 60,569 pcs*

- name, address, postal code, city, country, e-mail address, telephone number, language, account number

- personal identity code of 24,315 data subjects

• Contact persons of businesses and company details, 5,707 pcs

- VAT ID, company name, address, postal code, city, country, language,

telephone number, e-mail address, credit ceiling and [redacted] *account manager*

• [redacted] *ERP user data, 1,800 pcs*

- name, e-mail address, telephone number, language, encrypted and salted password, country and team

• Contact information of contact persons of cities/municipalities, 1,383 pcs

- name, title, telephone number, e-mail address

• Web shop customers, 96,196 pcs

- e-mail address, encrypted and salted password and in some cases, name, telephone number and reference to customer data

The Request for consultation by the Office of the Data Protection Ombudsman states that "As a result of the data breach, a third party obtained the name, date of birth, personal identity code, and contact information of approximately 165,000 customers." in this regard, [redacted] *would like to make known that the numbers refer to the number of data subjects in each category with the categories overlapping to some degree. A data subject can belong to several groups: the data of some of the web shop customers, for example, is found in other customer data records. As a result, the actual number of data subjects is smaller than the combined number of all the groups mentioned above (165,655). The personal data categories similarly vary depending on the categories of data subjects. 24,315 data subjects were affected by a data breach involving their personal identity code.*

After the data breach, [redacted] took up extensive measures with the purpose of improving the information security of its systems and the data protection competence of its staff. In October 2020, the controller has commissioned an external expert to conduct a security test, which included system penetration testing. An external expert's assessment was that no vulnerabilities were found in the systems that could be exploited on the public network and that the targets to be tested were difficult targets for attackers due to effective attack prevention.

The controller has commented on the rapporteur's preliminary assessment, inter alia, as follows:

[--]

In connection with the previous project, the retention period for the data of landlords and occupants is set at 10 years from the end of the contract. *The data contains contact and identification information (name, contact information, personal identity code, account number).* [redacted] *wishes to furthermore state that the attacker has not gained access to guest data (guest data and customer data are kept separately, because guests are always private individuals whereas the customer is the person's employee or similar party).*

In the section of the facts in the Request for consultation (p. 5), the Office of the Data Protection Ombudsman claims that the controller has not indicated a clear, statutory need to keep the personal data for a period of 10 years. In this respect, [redacted] points out that in addition to the storage periods specifically laid down in legislation, the data storage period can be based on, simultaneously or additionally, to business needs. This is the case with [redacted]

[--]

When the storage periods were determined, the practical contents of the principles of storage period restrictions had not been fully determined, and in [redacted] view, the storage period of 10 years could be viewed reasonable when considering the quality of the data stored, needs of business operations, contractual obligations, and previous experiences on needing to retrieve old information. When defining the storage period, factors such as the expiry of liability for damages, as laid down in the Tort Liability Act, were also acknowledged. [redacted] states that it has had to retrieve old data in cases such as setting disputes in courts after the expiry of rental contracts, with lessors demanding compensation based on the condition of the apartment. In these circumstances, [redacted] has been obliged to retrieve information on guests who have strayed in the apartment to establish their observation on the state of the apartment during their accommodation ([redacted] rents apartments from their owners and gives access to them to the customers, so the actual guests can consist of, for example, the customer's employees).

After the re-examination to which [redacted] referred in its response, submitted to the Office of the Data Protection Ombudsman on 14 August 2020, [redacted] has further specified and restricted the storage periods based on the types of data contained.

Regarding the data minimisation principle, the request for consultation does not specify the extent to which the Office of the Data Protection Ombudsman finds that the data processed is not adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. The view of [redacted] is that the contractual data are necessary with regard of the purposes of processing (apartment rental, offering accommodation services, compliance with statutory obligations and contract obligations).

To the extent provided for in Article 25(2) of the GDPR, [redacted] states that the personal data breach at issue is not the result of the default access of personal data to an unlimited number of persons, as described in the request for consultation. According to the controller:

The attacker has gained access to personal data following a cyber-attack (i.e., criminal activity) by taking advantage of the vulnerability of a single interface. The information has not been freely available, and they were accessed following a cyber-attack. The interface that was used as the attack vector has, in the manner described in the data breach, been linked to an extranet used by [redacted] customers which was open to the public due to this reason.

The personal data has become accessible to the single attacker following the attack. [redacted] is not aware of the attacker making the data available for unlimited access. Thus, [redacted] regards that [redacted] has not made the personal data accessible to an indefinite number of natural persons as laid down in Article 25(2) of GDPR. To prevent the data in question made accessible to an indefinite number of natural persons, [redacted] had implemented technical and organisational measures to protect the systems and the data contained within even before the data breach.

Regarding the provisions of point (d) of GDPR Article 32(1) and Article 32(2), [redacted] states that the attack that caused the data breach reviewed here was targeted against [redacted] extranet service (i.e., the self-service portal for [redacted] customers) and the interface linked to its ERP system. Extranet is used by [redacted] customers, so it must be made available on public Internet. There are other public interfaces linked to the ERP, including external services

(Oikotie etc). In the other interfaces of the system, an input check exists to block SQL injections, but in this interface the input check had been left out due to an earlier error, which resulted in the vulnerability. Even before the data breach reviewed here, [redacted] has implemented several technical and organisational measures to ensure information security. The application development complies with [redacted] application development process and [redacted] Privacy by Design Policy. The services offered by the Amazon Web Services (AWS) platform are used alongside [redacted] own technical safeguards. In information security measures, [redacted] has worked with external service providers even before the data breach. One example of this is the external audit of the source code that was carried out in 2018. Organisational security measures (including regular reviews of log data) helped to detect the attack while it was still ongoing and to stop it.

As a conclusion, [redacted] states that a single vulnerability of an interface that must be made accessible on public internet because of its purpose of use, was the root cause of the data breach. Before the data breach, [redacted] has attempted to implement sufficient technical and organisational safeguards to protect personal data. [redacted] has similarly sought to ensure the sufficiency of these measures in accordance with point (d) of Article 32(1) of the GDPR, as referred to in the Request for consultation by the Office of the Data Protection Ombudsman, with measures such as the code analysis by an external expert (referred to above) and an internal review of source code in connection to the application development process. An information security audit was carried out by an external expert after the data breach, and its conclusions similarly indicate that information security measures have been implemented, as no similar or other types of security vulnerabilities in the public network were detected of which advantage could be taken. Therefore, [redacted] finds that it has taken appropriate technical and organisational measures to safeguard data as laid down in Article 32 of the GDPR.

Above, the personal data breach has been reviewed mostly from the perspective of GDPR's point (d) of Article 83(2) and the technical and organisational measures implemented. About the other factors as laid down in Article 83(2), [redacted] concludes the following.

[redacted] detected the data breach itself and corrected the vulnerability instantly, which restricted the extent of the data breach. [redacted] informed both the Office of the Data Protection Ombudsman and the data subjects independently and has engaged in active cooperation with the National Cyber Security Centre and the police in the investigation of the attack. [redacted] has allocated significant resources for the investigation and audit work following the data breach and reviewed its entire IT infrastructure to detect any similar and equivalent vulnerabilities in the aforementioned manner.

[--]

The cross-border nature of the case

The processing of cases that are cross-border as defined in Article 4(23) GDPR. Such cases shall be dealt with in accordance with Article 56 and Chapter VII of the GDPR.

On 13 August 2020, the controller was asked to clarify the possible cross-border nature of the case. The controller submitted clarification on 30 August 2020. The controller has stated in its statement that it will act as a controller with regard to the processing of personal data in question. The controller operates in Finland, Sweden, Denmark and Norway. According to the controller, the data are processed in the group's common customer information system. The controller states that the main establishment is in Finland and that the Finnish office takes decisions on the processing of personal data at issue. Therefore, the Office of the Data Protection Ombudsman has been considered competent to deal with the case as the lead supervisory authority. In accordance with the procedure laid down in Article 60 GDPR, the Office of the

Data Protection Ombudsman has dealt with the matter in cooperation with the supervisory authorities of the participating Member States.

On 29 October 2020, the Office of the Data Protection Ombudsman provided relevant information to other supervisory authorities in accordance with Articles 56 and 60(3) of the GDPR. The data protection supervisory authorities of the Land of Bavaria, Germany, Ireland, Poland, Norway, Lithuania, Spain, Latvia, Belgium, Bulgaria, France, Luxembourg, Hungary, Slovakia, Sweden, and Italy have indicated that they are participating supervisory authorities on the grounds that the processing of personal data in question affects or may affect data subjects in that Member State.

Handling of the case in the context of the cooperation procedure

On 24 August 2021, the draft decision of the Data Protection Ombudsman was submitted to the participating supervisory authorities for information pursuant to Article 60(3) of the GDPR. Office of the Data Protection Ombudsman received an objection to the draft from the Polish Supervisory Authority and comments from the supervisory authorities of Denmark, Hungary, and France.

In the view of the Polish Supervisory Authority, the draft decision of the Office of the Data Protection Ombudsman should be supplemented. According to the Polish Supervisory Authority, the decision should establish an infringement of Article 6(1) of the GDPR. The Polish Supervisory Authority also considered that Office of the Data Protection Ombudsman should provide the controller with a reprimand on an infringement of Articles 6 and 25(2) of the GDPR. The fact that the infringement has since been remedied is, in the view of the Polish Authority, irrelevant. In the view of the Polish Supervisory Authority, the reprimand would be necessary sanction to prevent possible future infringements. According to the Polish Authority, the imposition of a fine in addition to the reprimand would be proportionate, effective, and dissuasive. The non-application of a proportionate and effective remedy could, in the view of the Polish Supervisory Authority, lead to a lack of adequate warning to the controller against re-infringing the GDPR.

The Danish Supervisory Authority has requested that the assessment would be supplemented regarding the adequacy of the technical and organisational safeguards taken by the controller prior to the occurrence of a breach. The Hungarian Supervisory Authority concluded that the imposition of a penalty would not constitute a disproportionate penalty in relation to the infringements found in the decision. The French Authority has commented on its agreement to the draft decision.

On 27 May 27.5.2022, the Office of the Data Protection Ombudsman gave the controller the opportunity to comment on the comments and objections of the participating supervisory authorities. In this context, in addition to the factors already mentioned above, the controller has pointed out that it has made various improvements and enhancements to information security.

According to the controller, a long retention period had been decided on the basis of the limitation period of the right to compensation under the Damages Act. According to the registrar, long-term apartment rentals play an important role in its business, in which cases of damages may occur after a significant long term, apart from damage cases related to normal hotel operations. According to the controller, it has since, taking into account the opinion of the Data Protection Ombudsman, defined the retention period of customer data as the minimum retention period in the ERP system in accordance with the Accounting Act and has taken an informed business risk for itself in cases of damages that cannot be dealt with within this time limit.

According to the controller, the data breach mainly targeted customers who were active in the online service, and a minor amount of personal data was affected, for which the retention period in accordance with the Accounting Act had expired. The controller considers that the number of data subjects affected by the data breach would not have been substantially lower, even if there were retention periods in accordance with the current specifications.

According to the controller, it detected the breach itself and corrected the vulnerability immediately, which was able to limit the extent of the breach. According to the controller, it reported the breach on its own initiative both to the Office of the Data Protection Ombudsman and to the data subjects and has also actively cooperated with the Cybersecurity Centre and the police in the investigation of the attack. According to the controller, it has allocated significant resources to the post-security breach investigation and investigation and has reviewed the entire IT infrastructure for similar and other vulnerabilities as described in this and the previous counterpart. The controller considers that the imposition of a penalty would be disproportionate in relation to the infringements found.

Office of the Data Protection Ombudsman has partially considered the objection raised by the Polish Supervisory Authority in his decision and added infringements of Article 25(2), Article 32(1)(d) and (2) to the decision. Following the Danish Supervisory Authority's comment, the Data Protection Ombudsman decision complemented the assessment of the safeguards and found that the safeguards were not sufficient as required by Articles 25(2), 32(1)(d) and (2). In accordance with Article 60(5) of the GDPR, the Office of the Data Protection Ombudsman has submitted a revised draft decision to the participating supervisory authorities.

None of the participating supervisory authorities has submitted a meaningful and reasoned objection to the revised draft decision of the Data Protection Ombudsman by 15 February 2023. The final decision shall be notified to the controller, the complainants, and the participating supervisory authorities.

Applicable legislation

The General Data Protection Regulation of the European Parliament and of the Council (EU 2016/679, the GDPR) has been applied as of 25 May 2018. As a regulation, the GDPR applies directly in Member States. The GDPR is supplemented by the Finnish Data Protection Act (no. 1050/2018) that has been in force since 1 January 2019. The Data Protection Act repealed the Personal Data Act (523/1999).

The GDPR is applied to this case.

Legal issues

The Data Protection Ombudsman assesses and decides the matter based on the General Data Protection Regulation (EU) 2016/679. The questions under review in this matter:

1) Has the controller conformed with the principle of data minimization as laid down in point (c) of Article 5(1) of the GDPR and the principle of storage limitation of point (e) of Article 5(1) as it has stored the personal data of data subjects for a period of 10 years?

2) Has the controller conformed with its responsibility, laid down in Article 25(2) of the GDPR, to implement appropriate technical and organizational measures used to ensure that, by default, personal data are not made accessible to an indefinite number of natural persons and that the storage period of the data is restricted?

3) Has the controller conformed with the provisions on the testing and assessing the appropriate level of security as laid down in point (d) of Article 32(1) and Article 32(2) of the GDPR?

If the processing of personal data does not meet the provisions, a ruling must be given on the sanctions to be imposed on the controller.

Decision of the Data Protection Ombudsman

In his decision, the Data Protection Ombudsman considers that:

1. The Data Protection Ombudsman finds that the controller has not conformed with the principle of data minimisation as laid down in point (c) of Article 5(1) of the GDPR and the principle of storage limitation of point (e) of Article 5(1) as it has stored the personal data of data subjects for 10 years. The Data Protection Ombudsman furthermore finds that the controller has not conformed with its responsibility, laid down in Article 25(2) of the GDPR, to implement appropriate technical and organisational measures used to ensure that the data is only stored for a period that is necessary.

2. The Data Protection Ombudsman considers that, in the event of a breach described, the controller had not complied with its obligation under Article 25(2) of the GDPR to take appropriate technical and organisational measures to ensure, in particular, that personal data are not made available by default to an unlimited number of persons.

3. The Data Protection Ombudsman considers that, in the event of a breach, the controller had not complied with the obligations laid down in Article 32(1)(d) and (2) GDPR to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Order

The Data Protection Ombudsman shall issue an order to the controller pursuant to Article 58(2)(d) of the GDPR to assess which personal data must be retained in order to comply with the obligations laid down in the Accounting Act with regard to the personal data processed. In so far as the data do not need to be stored to comply with accounting or other legal obligations, the Data Protection Ombudsman orders the controller to shorten the processing time of the personal data.

Reprimand

The Data Protection Ombudsman shall issue a reprimand to the controller pursuant to Article 58(2)(b) GDPR. The Data Protection Ombudsman points out that, in the event of a breach, the controller did not comply with the obligations of design and by default (Article 25(2) GDPR) and the obligation to adequately protect personal data (Article 32(1)(d) and (2) GDPR).

Reasoning

Principle of data minimisation

The principle of data minimisation is laid down in point (c) of Article 5(1) of the GDPR. Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

The personal data that are processed must be relevant in relation to the purposes for which they are processed, as mentioned above. The Government proposal on the old Personal Data Act also specified the contents of what is known as the Principle of Necessity. Personal data can be regarded necessary for the purpose of processing when they are adequate and relevant and not extensive for the purpose they are collected and later processed (Government proposal 96/1998 vp, p. 42). Similarly, Recital 39 of the GDPR states that personal data must be adequate, relevant and limited to what is necessary for the purposes for which they are processed. Therefore, it can be stated that personal data can only be processed if the purpose of processing cannot be reasonably achieved with other means.

The European Data Protection Board has included advice on the data minimisation principle in the guidelines it has published[2]. These guidelines indicate that it must be established first if the processing of personal data is, in fact, necessary. It is specifically stated that processing of personal data shall be altogether avoided when this is possible. It is furthermore emphasised that the personal data processed shall be relevant to the processing in question. All personal data shall be necessary for the specified purposes. Each personal data element should only be processed if it is not possible to fulfil the purpose by other means.[3] Therefore, only the minimum amount of personal data necessary must be collected.

Principle of storage limitation

The principle of storage limitation is laid down in the GDPR, point (e) of Article 5(1). Personal data must be kept in a form which only permits the identification of data subjects for as long as is necessary for the purposes of processing the personal data. This means that personal data storage period must be as short as possible. Recital 39 of the GDPR states that personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. This means that it must be ensured that the period for which the personal data are stored is limited to a strict minimum. Recital 65 of the GDPR states that a data subject should have the 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation.

About the matter reviewed

The controller has stored personal data of customers for up to ten years after the expiry of the rental contract. The controller has justified the storage period with business needs, as it has had to retrieve old data in cases such as setting disputes in courts after the expiry of rental contracts, with lessors demanding compensation based on the condition of the apartment.

However, it seems evident that conflicts are primarily addressed soon after the rental period ends, and in these cases, the relevant data could be stored for a longer period, if necessary, than data of customer relationships that are not sources of dispute. The controller has therefore not been able to present sufficient evidence as to why personal data from apartment rentals should be stored for ten years by default.

In the last consultation, the controller has stated that it has reduced the retention period after the breach. According to the controller, it has defined the retention period of customer data as the minimum retention period in the ERP system in accordance with the Accounting Act and

[2] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (issued on 13/11/2019).
[3] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (issued on 13/11/2019) p. 19.

has taken an informed business risk to itself in relation to damages cases that cannot be processed within this time limit.

Under Chapter 2, Section 10(1) of the Accounting Act (1336/1997), the financial statements, the annual report, the accounting records, the list of accounts and the list of accounts and materials must be kept for at least 10 years from the end of the financial year. Further, in accordance with Chapter 2, Section 10(2) of the Accounting Act, unless a longer period for retention is laid down elsewhere in the Act, supporting documents for the financial year, correspondence relating to transactions and other accounting records other than those referred to in subsection 1 must be kept for at least six years from the end of the year in which the financial year ended.

Chapter 2, Section 5 of the Accounting Act provides for a voucher. Voucher means a dated and individualised written expression of the transaction, such as a receipt. As regards the definition of correspondence relating to transactions, the Board of Directors, for its part, refers to the Accounting Board's Guideline of 1 February 1.2.2011 on accounting methods and records, in which it is stated in section 4.2 that correspondence relating to transactions is documents other than supporting documents in the accounting records. Such material includes, for example, declarations made based on accounting by public authorities (e.g., tax returns) and declarations made to pension insurance corporations or other entities and other statutory declarations (HE 89/2015 vp, p. 49).

The controller has not provided any further explanation as to which accommodation and tenancy data the retention period determined based on the Accounting Act applies. However, based on the above legal provisions, it is clear that not all information on accommodation and rental relationships can be considered as data within the meaning of Chapter 2, Section 10 of the Accounting Act. [4] The controller has not provided a clear justification as to why a retention period based on the Accounting Act applies to all personal data relating to accommodation and apartment rentals.

Based on the above, the Data Protection Ombudsman considers that the controller has not complied with Article 5(1)(c) and (e) of the GDPR in its processing operations concerning data retention.

Data protection by design and by default

Article 25(2) of the GDPR requires that the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that personal data are not made accessible by default and without the individual's intervention to an indefinite number of natural persons.

Security of processing

By virtue of point (d) of Article 32(1) of the GDPR:

"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

[4] See, for example, Decision No 4359/163/2018 of the Deputy Data Protection Ombudsman

[--]

d) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."

By virtue of Article 32(2) of the GDPR:

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

The processing of personal data must be confidential and secure. The controller is required to assess the potential risks, the level of the organisation's data protection and data security guidelines, and the technical security of personal data. The adequacy of safeguards must be weighed against the circumstances and risks.

The purpose of safeguards is to ensure the confidentiality, integrity and availability of systems, services and data. Personal data must be protected against unauthorised and unlawful processing, and from accidental loss, destruction or damage. Personal data breaches can cause significant risks to data subjects, such as falling victim to identity theft or fraud. Personal data must be protected during all processing operations and for the entire lifespan of processing.

The controller must regularly test the functionality of safeguards and make the required improvements.

About the matter reviewed

Based on the explanation provided, the controller considers that it has taken appropriate technical and organisational measures to protect the data in accordance with Article 32 of the GDPR. According to the report provided by the controller, it had in place, inter alia, the following safeguards:

- The data is transferred via a secure HTTP connection from the user to the registrar's servers.
- The data is stored in encrypted databases and log files, accessed by a limited number of persons.
- In addition to the controller's own measures, the technical safeguards utilise the services provided by the Amazon Web Services (AWS) platform.
- Other interfaces of the system include a feed check to prevent SQL injections (the input check had been omitted from the interface used in the attack due to a previous error, resulting in a vulnerability).
- In its application development, the controller follows the application development process and the privacy by design policy.
- The application development process involves reviewing the source code.
- Prior to the breach, the controller has made use of external experts, for example in relation to an external audit commissioned for source code in 2018.

According to the controller, after the breach, it commissioned an external expert to conduct a security audit that did not identify similar or other exploitable vulnerabilities open to the public network.

This data breach was carried out using a SQL injection. A SQL injection means that random commands are used to alter the contents of the database environment in use. The attack can be carried out by taking advantage of source data checks that are not sufficient or do not work

properly, and in some cases through incorrect processing of data in the data base directly in the interface.

SQL injections are a widely known information security risk, so it is important that the system administrations of database servers protect themselves with appropriate information security measures.[5] In the prevention of SQL injections, the minimum level to ensure is that system testing takes place, and extensive firewall systems can be used to prevent injections in online applications. The system attacked here was an extranet application, i.e. a self-service portal for customers, which means that it is not feasible to prevent using it on public internet as customers could no loner use the service. According to the controller, the source code was audited in 2018. The Data Protection Ombudsman has considered that the audit took place two years before the breach, and the controller has not indicated that it had carried out penetration testing or audits since 2018.

The controller has stated in its report that, after a breach of security, it has commissioned a penetration test for its systems by an external expert. No vulnerabilities that could be exploited on the public network were found in this test. If the controller had carried out penetration testing before the incident occurred, the vulnerability exploited in the breach could possibly have been detected. As mentioned above, SQL injections are one of the most critical security risks for online applications. The controller could have performed more regular testing to detect and correct vulnerabilities. Therefore, the Data Protection Ombudsman considers that the controller had not carried out adequate procedures to ensure a level of security corresponding to the risk as required by Article 32(1)(d).

Applicable legal provisions

As set out in decision.

Appeals

According to Section 25 of the Data Protection Act (1050/2018), this decision may be appealed in the Administrative Court by lodging an appeal in accordance with the provisions of the Administrative Judicial Procedure Act (808/2019). Appeals shall be lodged in the Helsinki Administrative Court.

The appeal instructions are enclosed.

The Service of notice

Notice of this decision will be served by post against an acknowledgment of receipt pursuant to section 60 of the Administrative Procedure Act (434/2003).

For more information on this decision, please contact the rapporteur

Senior Officer

Data Protection Ombudsman _____

[5]OWASP, an international organisation dedicated to web application security, has rated injections as the most significant risk. See https://owasp.org/www-project-top-ten/ Accessed 21 December 2022

Senior Officer _____

The document is signed electronically. The authenticity of the signature can, if necessary check with the Registry of the Office of the Data Protection Ombudsman.

Appendices

Appeal instructions

Distribution

Accommodation service [redacted]

Complainants

Contact information of the Office of the Data Protection Ombudsman

Postal address: PO Box 800, 00531 Helsinki

E-mail address: tietosuoja@om.fi

Telephone gearbox: 029 566 6700

Webpages: www.tietosuoja.fi