Complainants
See Annexes 1-4

Subject of supervision
Easypark AB

Reference number:
DI-2022-1441

Date:
2025-04-25

Decision following supervision under the General Data Protection Regulation – Easypark AB

Decision of the Privacy Protection Authority

The Swedish Authority for Privacy protection (IMY) notes that Easypark AB, (company registration number 556626-7893), has processed personal data in breach of Article 32(1) of the GDPR[1] by failing to take appropriate technical measures during the period January 2018 to July 2020, thereby enabling unauthorised access to the personal data of its customers.

The Swedish Authority for Privacy Protection issues a reprimand to Easypark AB pursuant to Article 58(2)(b) GDPR for the infringement of Article 32(1) GDPR.

Presentation of the supervisory case

Processing

IMY has initiated supervision of Easypark AB (Easypark) in relation to four complaints concerning the security of the processing of personal data. The complaints have been submitted to IMY, as the lead supervisory authority for Easypark's activities under Article 56 GDPR, by the supervisory authorities of the countries where the complainants have lodged their complaints (Denmark and Iceland). The transmission has taken place in accordance with the provisions in the GDPR on cooperation in cross-border processing.

Due to the cross-border nature of the case, IMY has made use of the cooperation and consistency mechanisms provided for in Chapter VII of the GDPR. The data protection authorities of Germany (Baden-Württemberg), Denmark, Italy, Norway, Hungary, France, Slovenia, Germany (Mecklenburg-Vorpommern), Austria, Germany (Berlin), Germany (Lower Saxony), Germany (Bavaria - public sector), Finland, Spain and Iceland have indicated that they are the supervisory authorities concerned.

The complaints in the case have in common that they concern security in the processing of personal data. IMY has therefore limited supervision to whether Easypark, with regard to the processing of each of the complainants' personal data,

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Postal address:
Box 8114
104 20 Stockholm
Website:
www.imy.se
E-mail:
imy@imy.se
Telephone:
08-657 61 00

has taken sufficient measures to ensure a level of security appropriate under Article 32 of the GDPR.

The proceedings before IMY were conducted by exchange of letters.

The complaints

The complaints essentially state the following.

Complaint 1 (Denmark with national registration number 2020-7320-2103, complainant "JL")
The complainant was contacted by a person who stated that he had paid for the complainant's parking through the Easypark app. That person had access to the complainant's Easypark account and, therefore, to the personal data stored in that account.

Complaint 2 (Denmark with national registration number 2020-7320-2103, complainant "RA")
The complainant has been charged for another person's car parks made through the Easypark app. That person had access to the complainant's account and was able to add details of his own car to that account and, in connection with parking, to pay using the complainant's PayPal account. The person also had access to the complainant's account history. Complaints 2 and 3 relate to the same event.

Complaint 3 (Denmark with national registration number 2020-7320-2103, complainant 'MH')
A person had access to the complainant's Easypark account, which enabled him to stop the complainant's ongoing parking. That person informed the complainant that his account had been debited for the complainant's parking. The fact that the parking was stopped resulted in the complainant receiving a parking fine which he had asked Easypark to remove. Complaints 2 and 3 relate to the same event.

Complaint 4 (from Iceland with national registration number 2020072096)
The complainant used the Leggja parking app in the past but started using the Easypark app after Leggja's services were transferred there. Shortly after logging into the Leggja app and transferring his data to Easypark, the complainant received a call from a colleague who stated that she had access to the complainant's data, including his credit card information, in her own Easypark app.

What Easypark has stated

In summary, Easypark states the following.

Complaints 1-3
Background
Easypark AB and Easypark A/S are joint controllers of the personal data processing described in the complaints.

Easypark provides a mobile application that allows customers to manage their parking and pay for parking services via a smartphone (the 'Parking App'). A customer registers for the service by entering their phone number in the Parking app. If the given telephone number is not previously registered with Easypark, a new account is created in the Parking app, which is linked to the given telephone number. When registering an

account, the customer must accept the general terms and conditions for the Parking App. Once an account has been registered, the Customer can add registration numbers to the Parking App for the vehicles for which the Customer wishes to administer parking and a payment method.

If the telephone number entered in the Parking App is already registered to an account with Easypark, this has been perceived by the Parking App as a login attempt to that account instead of a registration of a new account. In this case, a PIN code has been sent via text message to the given phone number. To complete the login, the customer has then had to enter the PIN code in the Parking app. This has ensured that login has actually taken place from the phone associated with the phone number associated with the current account.

The customer's account in the Parking App is always linked to a specific phone number. In some cases, telephone numbers can be reused, for example, if the telephone operator assigns a telephone number to a new customer or if an employer assigns a telephone number previously held by one employee to another employee. Easypark has no legal or technical means to continuously check whether their customers change phone numbers. Easypark has therefore taken measures to prevent a phone number that a customer has registered in the Parking App from being used by other people to log in to the customer's account. One such measure is that it is specifically stated in the general terms and conditions of the Parking App that the customer is obliged to inform Easypark without delay if the customer's registered data has changed, e.g. if the customer changes mobile phone number. The customer can inform Easypark of this by changing the information via the company's website or by contacting Easypark's customer service.

In particular with regard to Complaint 1
It is true that another person had access to the complainant’s data. That person previously held the applicant’s telephone number.

On 27 February 2016, the person who obtained access to the complainant’s data registered a private account in the Parking App. At the time of registration, he gave a telephone number which had been assigned to him by his employer. In doing so, he approved the general terms and conditions of service. He terminated his employment on 30 September 2017 and, on 19 October 2018, registered another private account with Easypark linked to a new telephone number. However, he did not close the old account or notify Easypark of changes to his details.

Thereafter, the complainant was assigned, through the same employer, the telephone number previously held by that person. The complainant logged into the Parking App using that telephone number and was then logged into the existing account registered with another person. At that stage, the complainant was logged in to the account, since the PIN code confirming that the account was connected to the telephone was sent by text message to the telephone number that was now his. The Complainant did not change the information contained in the account (e.g. name, address, telephone number or selected payment method) but added its own vehicles and subsequently started using the payment method that the previous holder of the telephone number had registered in the account to pay for parking services using the Parking App. The account continued to be used until 7 February 2020.

The previous holder of the telephone number contacted Easypark on 8 January 2020 requesting the parking history of the account. As the account was still registered in his

name, Easypark provided him with the parking history of the account. He then became aware that payments for parking had been made through the account with the telephone number in question without his knowledge, even though the account was registered in his name. It was only at that time that he informed Easypark that the telephone number had been transferred to another employee of his former employer.

Later that day, on 8 January 2020, the complainant contacted Easypark and asked the company to provide him with all the details of the account. Easypark did not disclose the information to the complainant because the account was not registered in the complainant's name. In the light of the above, Easypark closed the account linked to the telephone number in question on 13 January 2020. Later that day, Easypark sent the complainant an email informing it that the account was not registered in the complainant's name and that, as a result of the data protection legislation, it was prevented from disclosing the requested data to the complainant, that the previous holder of the telephone number had not changed the telephone number associated with the account or deleted the account even though he was required to do so, that Easypark could not know that the customer's data had changed if the customer did not inform Easypark of this, that the account was closed and that, if the complainant wished to continue using the Parking App, he would have to register a new account.

In conclusion, it must be held that the event complained of was caused by the fact that, contrary to the general terms and conditions, the former holder of the telephone number failed to inform Easypark that he had changed his telephone number, that the complainant chose to use an account registered in the name of another person, and that the complainant did not change the payment method for the account, but chose to pay for parking services using the payment method that another person had linked to the account.

The unauthorised access to the complainant's data was remedied by the closure of the account at issue by Easypark on 13 January 2020.

In particular with regard to Complaint 2
It is true that another person had access to the complainant's data. That person had taken over a telephone number previously used by the complainant.

On 12 October 2015, the complainant registered a private account in the Parking App. It seems clear that the complainant had been assigned that telephone number by his employer. When registering the account, the complainant accepted the general terms and conditions of the Parking App.

On 1 March 2018, the complainant ceased to have access to the telephone number on which the account was registered, but did not inform Easypark thereof. Instead, the complainant continued to use the account and also created a new account with Easypark.

Another person was assigned the complainant's previous telephone number in January 2020 and logged into the Parking App using that telephone number on 15 February 2020. The person was logged into the account registered by the complainant because the PIN code confirming that the account is linked to the phone was sent by text message to the phone number on which the account was registered. The person did not change the information held in the account (e.g. name, address or chosen payment method) but added his own vehicle and then started using the payment method registered by the complainant in the account to pay for parking services with the Parking App. In that context, the complainant, who was therefore still using the account in question, noted that he was paying for parking through that account. When

the complainant discovered this, the complainant stopped the parking. The complainant then called the new holder of the telephone number and informed him that he had stopped the parking and that a certain amount had been charged to the complainant. The new holder of the telephone number then changed the details of the complainant held in the account by replacing them with their own details (e.g. name, address and method of payment chosen).

The complainant contacted Easypark on 18 February 2020. On 18 February 2020, in the light of the information received from the complainant, Easypark terminated the account linked to the telephone number in question.

In conclusion, the incident complained of was caused by the fact that, contrary to the general terms and conditions of the Parking App, the complainant failed to inform Easypark that he was no longer using the telephone number to which the account was linked and that the new holder of the telephone number chose to use an account registered in the complainant's name and to pay for parking services using the payment method linked to the account by the complainant.

The unauthorised access to the complainant's data was remedied by the closure of the account at issue by Easypark on 18 February 2020.

In particular with regard to complaint 3
For the sake of clarity, Easypark would like to point out that complaints 2 and 3 concern the same event.

It is true that another person had access to the complainant's data. This person is the same as the complainant in complaint 2. That person previously held the complainant's telephone number. With regard to the description of the course of events, reference is made to what Easypark stated above under the heading 'Specific *complaint 2'.* The complainant in complaint 3 is the person who took over the telephone number from the complainant in complaint 2.
The unauthorised access to the complainant's data was remedied by the closure of the account at issue by Easypark on 18 February 2020.

Common to complaints 1-3
Easypark has fulfilled its obligations to ensure that personal data is processed in a manner that complies with the General Data Protection Regulation. However, Easypark wishes to point out that, in the period following the incident, it has taken steps to further ensure that an event of the kind complained of does not occur.

Easypark would also like to point out that it must have been particularly clear to the previous holders of the telephone number (including the complainant 2) that they had an obligation to inform Easypark that the telephone number no longer belonged to them, as this was expressly stated in the general terms and conditions of the Parking App and the telephone number was used to log in to the Parking App. Furthermore, it must have been particularly clear to the person who took over the telephone number (including Complainant 1 and Complainant 3) that the account to which he logged in belonged to another person, as this was apparent from the information in the account.

The data of the complainant covered by the unauthorised access was of limited sensitivity. As regards complaint 1, it included the telephone number, the registration number of the vehicle, the start and end time of the parking and the parking area code. With regard to complaint 2, it included the name, address, e-mail address, vehicle registration number, parking start and end time, parking area code and the chosen payment method (in this case that PayPal was selected, but no details regarding the

account). As regards complaint 3, it included the address, e-mail address, telephone number, vehicle registration number, parking start and end time, parking area code and payment method (in this case the card issuer and the last four digits of the card number).

The location data processed in the Parking App includes a specific geographical location that is limited in time and is only intended to enable the customer to park in a specific parking space for a certain period of time. Such data is processed while the customer is parking and stored in the Parking App as a transaction in the customer's parking history. The area code refers to a specific area for parking (which can be of varying sizes) and does not mean that the customer's GPS coordinates or other detailed information about the customer's location is shown in the user interface in the Parking app.

Furthermore, there has been a very limited dissemination of a small number of personal data where only one third party has had access to the personal data. Nor was it possible for the event to take place in an easy manner, since the unauthorised access was caused by the fact that the original account holder did not deregister the telephone number in question when it ceased to use the number, contrary to the applicable conditions in the user agreement, and that the number was subsequently reused. It is therefore an event that concerns only one reused telephone number and where only one other person has been able to access an account in the Parking App through PIN verification.

Furthermore, the parking app has a limited area of use as it only allows the data subjects to manage parking and pay for Easypark's parking services. The data subjects are Easypark's customers and they are not in a vulnerable or exposed position vis-à-vis Easypark. The risk associated with the personal data processing in the Parking App and the unauthorised access is therefore very low.

Easypark's assessments regarding the appropriate level of security regarding complaints 1-3
Easypark considers that the processing of personal data has been in accordance with the requirements for appropriate security measures in the General Data Protection Regulation. Easypark works continuously to ensure that appropriate technical and organizational measures are taken during personal data processing, including protection against unlawful or unauthorized processing and against accidental loss, destruction or damage. This means that, in accordance with Article 24(1) of the GDPR, Easypark continuously reviews, develops and updates its technical and organisational measures.

Easypark considers that it would not have been appropriate to verify on an ongoing basis that each customer still held the telephone number linked to the customer’s account, as this would entail extensive processing of personal data which, in itself, would risk being in breach of several provisions of the GDPR. Furthermore, giving the customer responsibility for keeping his or her personal data up-to-date and correct is considered to comply with the principle of accuracy under Article 5(1)(d) of the GDPR, whereby the company’s decision to impose this responsibility on the customer is an example of the controller taking all reasonable steps to ensure that the personal data being processed are correct.

When developing the Parking App, Easypark made the assessment that the personal data processing in the Parking App would not likely lead to a high risk to the rights and

freedoms of data subjects. On that basis, Easypark considered that the technical and organisational measures it took in relation to the personal data processed were appropriate and proportionate to the limited risks for the data subjects.

Easypark has intended to provide a smooth, simple and user-friendly service and balance the requirements of the General Data Protection Regulation on, inter alia, privacy and confidentiality as well as technical and organisational measures with the requirements of data minimisation and accuracy. In balancing those interests, at the time of the incident to which the complaints relate, Easypark considered that there was no basis under the GDPR for it to collect more personal data about customers than those necessary to verify and log in customers securely and to provide the functionalities of the service. This assessment was made in the light of the action Easypark decided to take vis-à-vis customers, i.e. that, by accepting the General Terms and Conditions, customers accept a responsibility to keep the telephone number updated during the term of the contract. Easypark's overall assessment was that the contractual obligation for the data subject to update his or her telephone number in conjunction with the PIN verification and other technical and organisational measures constituted appropriate measures to ensure adequate security of the personal data processed in relation to the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks for the data subject.

In light of the fact that there have been incidents with customer verification, Easypark has begun work on identifying additional layers of protection for customer verification. A new solution was implemented in 2019 in one market, but was later removed as it did not work as expected. The project was postponed in the context of the COVID-19 pandemic, but the work resumed in October 2020 and was launched in 2021.

The new solution for customer verification essentially means that Easypark in the Parking app applies so-called multi-factor authentication when logging in. The new solution means that several layers of protection are applied to verify the customer's identity when logging in and means that it is not possible to access an account at Easypark by only having access to a phone number.

Complaint 4
Easypark AB and EasyPark Ísland ehf are joint controllers of the personal data processing described in the complaint.

It is true that another person, the complainant's colleague, had access to data relating to the complainant. The access was caused by an incorrect matching of so-called 'digital fingerprints' in connection with the migration of the complainant's and his colleague's accounts with the Icelandic company Já hf (with the Leggja app) to Easypark's system, following Easypark's acquisition of Já hf's business. A digital fingerprint consists of a large number of parameters related to the customer at a specific time, such as IP address, phone model and operating system. The error was due to a series of unusual factors, in which the complainant and his colleague initiated account migrations at the same time, while being connected to the same WiFi network (and therefore using the same IP address). As a result, the complainant's account has been visible to his colleague.

In that regard, Easypark notes that the incident is the only one of its kind which it has experienced in the application of the migration flow. Easypark has applied the migration flow to a number of acquisition-related transfers preceding the event

complained of. To the best of their knowledge, no such incident has ever occurred before or since.

The data of the complainant covered by the unauthorised access was of limited sensitivity. The categories of the complainant's data covered by the access were name, address, e-mail address, Icelandic personal identity number, telephone number, vehicle registration number and details of the payment method (in this case, the card issuer and the last four digits of the card number).

There has been a very limited dissemination of a small number of personal data where only one trusted third party, the complainant's colleague, has had access to the personal data. Nor has it been possible for the incident to take place in an easy way, as the unauthorised access has occurred due to a very rare deviation in the migration flow. It was therefore an event which could not have been foreseen by Easypark, since, first, the detailed tests and checks of the migration flow carried out by Easypark before the migration did not indicate that such an event could occur and, second, no similar event had, to the best of their knowledge, occurred at any earlier or later time when Easypark carried out account migrations. Easypark would also point out that it is very unlikely that an event such as that complained of could cause several persons to have unauthorised access to a customer's account, since that would presuppose that all the special and interrelated causes giving rise to the event were present at the same time in relation to several persons.

The migration flow applied in connection with the event complained of was one of Easypark's proven model for account migrations. The migration flow was designed in a well-thought-out manner, taking into account in particular the latest developments, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks for the data subjects. Of course, it was also important for Easypark that the migration flow as well as previous account migrations performed by Easypark were carried out in a safe manner so as not to cause inconvenience to Easypark's prospective customers.

To achieve a secure solution, Easypark took several measures, such as using a digital fingerprint solution containing a large number of parameters and ensuring that all tokens and links had a short lifespan. Furthermore, tests and checks of the migration flow were carried out to ensure that this functioned as intended before the migration of the accounts from Leggja to Easypark was carried out.

After becoming aware of the incident complained of, Easypark also undertook an investigation to identify the reasons for the unauthorised access. During the investigation, Easypark repeatedly recreated the migration flow in a test environment without this resulting in anything other than error-free migration. After about two months of investigation, Easypark identified the reasons for the unauthorised access described above. The unauthorised access to the complainant's data has been rectified.

Easypark has decided to no longer use the migration flow used during the migration from Leggja and has therefore developed a completely new migration flow to avoid a risk of unauthorised access for the data subjects.

Reasons for the decision

Applicable provisions

According to Article 4(7) of the GDPR, the controller is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. The controller is responsible for and shall be able to demonstrate compliance with the fundamental principles set out in Article 5 of the GDPR. This follows from Article 5(2) of the GDPR.

It follows from Article 32(1) of the GDPR that the controller shall implement appropriate technical and organisational measures to ensure an appropriate level of security for the data processed. When assessing the appropriate technical and organisational measures, the controller shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks to the rights and freedoms of natural persons.

Pursuant to Article 32(1), appropriate safeguards include, where appropriate:
a) pseudonymisation and encryption of personal data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures to ensure the security of processing.

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

Member States may, in accordance with Article 87 of the GDPR, specify the specific conditions under which a national identification number or other generally accepted means of identification may be processed. In such cases, a national identification number or other recognised means of identification shall only be used under appropriate safeguards for the rights and freedoms of data subjects under this Regulation.

IMY’s assessment

The complaints and Easypark’s opinion on the matter have revealed that unauthorised persons have been given access to the complainants’ personal data in Easypark’s parking app. For complaints 1-3, this has been caused by the fact that the phone number that was linked to the parking account, and could be used for logging in to the parking app, was taken over by another user. For complaint 4, it was caused by two people migrating their previous Leggja accounts to the Eayspark parking app at the same time when they were connected to the same Wifi network.

Easypark is the data controller

Easypark has stated that Easypark and Easypark A/S are acting as joint controllers for the processing of personal data examined in complaint 1-3 and that Easypark and

EasyPark Island ehf are acting as joint controllers for the processing of personal data examined in complaint 4.

The investigation shows that Easypark provides the service that enables parking through the parking app and that involves the processing of customers' personal data. It is Easypark AB that has carried out the risk assessment of the processing of personal data and determined what measures were considered appropriate to take in relation to the personal data processing. IMY notes that Easypark AB has determined the purpose and means, i.e. how and why the personal data should be processed, for the personal data that is relevant in the investigation. It is therefore Easypark which, under Article 4(7) of the GDPR, is the controller of the processing of personal data in question.

Has Easypark implemented appropriate technical and organisational security measures?

The question that IMY has to consider is whether Easypark has taken appropriate technical and organisational security measures to protect the personal data processed taking into account the risks involved in the processing, in particular from unauthorised disclosure. The appropriate level of security shall be assessed taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons.

Complaints 1-3

The treatment has involved a risk
Easypark states that they considered that the sensitivity of the categories of personal data subject to unauthorised access was limited and that the risk associated with the processing was very low.

In complaints 1-3, in addition to information such as name, contact details and registration number, the unauthorized access has included location information, which has shown in which parking area the customer parked at the registered time. The data has thus shown in which area individuals have parked their car, when, and for how long.

Data showing geographical location may be of a privacy-sensitive nature as the data may reveal the movement patterns of data subjects[2]. For example, it may be possible to ascertain in which areas the data subject often parks at a certain time or whether a parking lot is located near a particular residential area, a hospital or a school. A parking area is a defined geographical area. Parking areas may vary in size. This means that the indication of the area code may in some cases lead to significant risks linked to the movement patterns of the data subject, while in other cases it is not possible or at least difficult to draw any conclusions about the movement patterns of the data subject based on the area code.

In conclusion, IMY considers that, in view of its nature, scope and context, the processing has entailed a risk that has led to a requirement for Easypark to ensure a level of protection that is appropriate in relation to the risk in question. The level of

[2] European Data Protection Board (EDPB) Guidelines 01/2020 on the processing of personal data in connection with connected vehicles and mobility-related applications Version 2.0 Adopted on 9 March 2021, section 2.1.1.

protection would ensure, inter alia, that personal data was protected against unauthorised access.

Easypark has not taken sufficient measures to protect the data
Easypark has assessed that the customer's acceptance of the general terms and conditions together with PIN verification to ensure that the person who logs in is also the one who has the phone number constituted appropriate security measures. The complaints and Easypark's statement show that, despite the measures taken, unauthorised persons have been granted access to the data.

IMY finds that the unauthorised access could have been prevented or at least made more difficult by additional security measures, such as, for example, multi-factor authentication. Easypark has stated that there have been incidents with customer verification that led them to start work on developing a new solution for customer verification in 2018.

According to IMY, there were shortcomings in the protection of personal data partly because Easypark did not take sufficient account of the risks posed by the processing when assessing the appropriate level of security and, partly because it did not take sufficient measures to ensure appropriate safeguards even though it was aware of incidents linked to customer verification.

In conclusion, IMY notes that Easypark has not taken sufficient technical and organisational measures to ensure a level of security appropriate to the risk involved in processing the personal data of the complainants referred to in Complaints 1-3. In those cases, Easypark therefore processed personal data in breach of Article 32(1) of the GDPR.

Complaint 4
The treatment has involved a risk
Easypark states that they considered that the sensitivity of the categories of personal data subject to unauthorised access was limited and that the risk associated with the processing was low.

In complaint 4, the data covered by the unauthorised access, in addition to data such as name, contact details and registration number, consisted of personal data that merited special protection, namely personal identity numbers, which may only be processed under certain conditions. IMY notes that this places higher demands on the level of protection and that the measures to ensure that personal data is protected against unauthorised disclosure and access must be adapted to the risk posed by the processing.

In conclusion, IMY considers that, in view of its nature, scope and context, the processing has entailed a risk that has led to a requirement for Easypark to ensure a level of protection that is appropriate in relation to the risk in question. The level of protection would ensure, inter alia, that personal data was protected against unauthorised access.

Easypark has not taken sufficient measures to protect the data
Easypark has assessed that the migration flow they applied at the time of transferring the customer's data from Leggja's app to Easypark's app had a suitable level of security. It is apparent from the complaint and Easypark's statement that an unauthorised person nevertheless obtained access to the applicant's data.

In the event of a transfer of customer data in connection with a company acquisition, it may be considered likely that there may be customers in the same workplace. Furthermore, it may be considered likely that these customers use the same Wi-Fi and the same type of work equipment, such as the same hardware and operating system. From the information provided by Easypark, it appears that none of the parameters used to create the digital fingerprint were unique to a specific user. IMY considers that the unauthorised access could have been prevented or at least made more difficult by additional security measures, for example by imposing a user interaction for identification in connection with the transfer of the data. Such a measure could, for example, have been the indication of the telephone number of the phone on which the data was transferred between the apps.

According to IMY, there were shortcomings in the protection of personal data, first, because Easypark did not take sufficient account of the risks posed by the processing to the personal data of data subjects when assessing the appropriate level of security and, second, because it did not take sufficient measures to ensure appropriate safeguards in connection with the transfer of the data.

IMY concludes that Easypark has not taken sufficient technical and organisational measures to ensure a level of security appropriate to the risk. Easypark has thus processed personal data in breach of Article 32(1) of the GDPR.

Choice of intervention

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that IMY has the power to impose administrative fines under Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or instead of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, it is clear from Article 83(2) which factors must be taken into account when deciding on an administrative fine and when determining the amount of the fine. In the case of a minor infringement, as set out in recital 148, instead of imposing a fine, IMY may issue a reprimand pursuant to Article 58(2)(b). Account shall be taken of aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and relevant previous infringements.

IMY has faound that Easypark has not taken sufficient technical and organisational measures to ensure a level of security appropriate to the risks and that Easypark has thereby processed personal data in breach of Article 32(1) of the GDPR.

The infringements found were caused by Easypark processing personal data with an insufficient level of security. These have been data with a relatively high protection value. However, the complaints relate to a limited number of cases where a few unauthorised persons have accessed a limited number of personal data. In cases where unauthorised persons have gained access to a person's personal data, this has been a distribution limited to only one other person. The unauthorised access was not due to a flaw in the open availability of the data online, but was connected solely to the possession of the telephone number used to create the original account. After the appellants contacted Easypark, Easypark immediately took steps to stop unauthorised access in the cases in question. After the events and before IMY began supervision, Easypark itself introduced changed procedures for logging in, which means that it is now not possible to access someone else's account simply by entering a phone number when logging in. The Company has not previously received any corrective

action for violation of data protection regulations. In those circumstances IMY finds that the infringements in question are such minor infringments within the meaning of recital 148 and that Eayspark must be given a reprimand under Article 58(2)(b) of the GDPR for the infringements found.

Annex

1. Complainant's personal data - complaint 1
2. Complainant's personal data - complaint 2
3. Complainant's personal data - complaint 3
4. Complainant's personal data - complaint 4

Copy to
Data Protection Officer