

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision 2022-05-13, no. DI-2021-6140. Only the Swedish version of the decision is deemed authentic.

Registration number:

DI-2021-6140 ,IMI. Case no.
186981, A60FD 399045

Decision under the General Data Protection Regulation– Volvo Personvagnar AB

Date of decision:

2022-05-13

Decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection (IMY) finds that Volvo Personvagnar AB has processed data in breach of

- Articles 12(3) of the General Data Protection Regulation (GDPR)¹ by not without undue delay responding to the complainant's request for access pursuant to Article 15 of GDPR, the 25 February 2020 only on 15 September 2021.

The Swedish Authority for Privacy Protection issues PUA a reprimand pursuant to Article 58(2)(b) of the GDPR for the infringement of Article 12(3) of the GDPR.

Report on the supervisory report

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding Volvo Personvagnar AB (the company) due to a complaint. The complaint has been submitted to IMY, as responsible supervisory authority for the company's operations pursuant to Article 56 of the General Data Protection Regulation (GDPR) from the supervisory authority in the Ireland where the complainant has lodged their complaint in accordance with the Regulation's provisions on cooperation in cross-border processing.

The investigation in the case has been carried out through correspondence. In the light of a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory authorities concerned have been the data protection authorities in Germany, Finland, France, Ireland, Italy, the Netherlands, Norway, Poland, Portugal and Hungary.

Postal address:

Box 8114
104 20 Stockholm

Website:

www.imy.se

E-mail:

imy@imy.se

Telephone:

08-657 61 00

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).

The complaint

In March 2019, the complainant requested access to his personal data pursuant to Article 15 of the GDPR. The applicant requested, inter alia, information on warranty repairs, carried out by a car brand repair shop belonging to the company (the car repair shop). The company replied that information on warranty was not available from the company.

What Volvo Personvagnar AB has stated

The company has mainly stated the following.

The company is the data controller for the processing to which the complaint relates.

On 25 February 2020, the complainant submitted a request for access to personal data. The request concerned, inter alia, an invitation to provide information on the servicing of the complainant's vehicle.

On 3 March 2020, the car repair shop sent the complainant a copy of a service invoice.

On 24 March 2020, the company sent a copy of the personal data containing information on the warranty repairs carried out, service on the vehicle and technical reports on the vehicle.

On 2 April 2020, the complainant lodged a complaint to the company alleging that the car repair shop had indicated that the information on the warranty repair, could not be disclosed.

On 14 April 2020, the complainant clearly stated that he wishes to have access to, inter alia, the following information:

- correspondence between the complainant and the company's customer service/carrier;
- correspondence between the complainant and the workshops concerning the vehicle in question;
- marketing; and
- recall of vehicles;

On 17 April 2020, the complainant received correspondence as set out above. At the same time, the company asked the complainant to clarify its request concerning marketing information and requests for correspondence with which country's customer service was the subject of the request.

On 14 May 2020, the complainant received a copy of the correspondence between the complainant, car repair shops and the company.

On 17 June 2020, the complainant requested information on warranty repairs from the company.

On 28 August 2020, a copy of the personal data was sent to the complainant with the following information on:

- correspondence from the company's customer service in the United Kingdom;
- correspondence from the local Irish sales office including, inter alia, the date of the warranty repairs carried out;

- service performed for which the company has information, the vehicle (date of technical reports on the vehicles); and
- a statement from a lawyer working for the company concerning what information the company doesn't have and that the applicant needs to contact the car repair shop concerned.

On 4 September 2020, the company informed the complainant that the company had requested the relevant car repair shop to provide information on service and warranty repairs.

On 15 September 2021, the DPO sent a letter to the complainant and apologised for the handling of the request for information on warranty repair. In its reply, the company attached the following information.

Data from the system QV90:

- service history (date, metering, workshop and dealer),
- roadside assistance insurance from the local system;
- the next service date according to service intervals;
- listing in free text about measures and warranty cases (date, metering, warranty case, so-called QB number), missing component, applied for costs from the workshop for work and materials, cost allocation (between sales company/importer and manufacturer).

Information from the system of technical records from the time when the complainant owned the vehicle, as follows:

- logs on the vehicle where it has been recorded in technical reports;
- possible warranty cases (errors/problems that may occur on this vehicle and on which it is possible to call for a guarantee);
- logs on completed warranty cases, reports such as problems with the vehicle where the workshop involves the support of the sales company and/or the support company. These reports are linked to the vehicle and the complainant.

The company submits that the car repair shops are independent of the company. It is the car repair shops that have carried out warranty and service work on the complainant's vehicles. It is for the car repair shops to provide the complainant with information on warranty and service work, as the workshops own the customer relationship and hold relevant information and data on such works. The complainant therefore needed to have a direct dialogue with the car repair shop on information concerning warranty and service provided. The company does not handle service or service invoices. Service is provided by the independent car repair shop and the car repair shop is data controller for the service information.

The company points out that the reason why the data from the QV90 system and the technical notes were not sent to when the complainant in the first communication was due to the human factor. The company has now ensured that the mistake will not happen again.

The company has been in constant communication with when the complainant and has attempted to respond to its various requests. The company points out when the complainant sought, in essence, information relating to the car repair invoice for a particular warranty and service work carried out, which is information to which the company did not have access to.

Justification of the decision

Applicable provisions, etc.

Concept of personal data

According to Article 4(1) of the GDPR, *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*

The concept of 'personal data' may include all information, whether objective or subjective, provided that it 'relates' to a particular person, which it does if, by virtue of its content, purpose or effect, it is linked to that person.²

In the judgment of the Court of Justice of the European Union in *Valsts ieņēmumu dienests*, the Court held that the information requested by the Latvian tax authority, in particular data relating to the chassis numbers of the vehicles advertised on the operator's web portal, constitutes personal data within the meaning of Article 4(1) of the GDPR.³

The European Data Protection Board (EDPB) Guidelines 01/2022 on data subject rights - Right of access, inter alia:

51. Additionally, the controller needs to assess whether the requests made by the requesting persons refer to all or parts of the information processed about them. Any limitation of the scope of a request to a specific provision of Art. 15 GDPR, made by the data subjects, must be clear and unambiguous. For example, if the data subjects require verbatim "information about the data processed in relation to them", the controller should assume that the data subjects intend to exercise their full right under Art. 15(1) – (2) GDPR. Such a request should not be interpreted as meaning that the data subjects wish to receive only the categories of personal data that are being processed and to waive their right to receive the information listed in Art. 15(1)(a) to (h). This would be different, for example, where the data subjects wish, with regard to data which they specify, to have access to the source or origin of the personal data or to the specified period of storage. In such a case the controller may limit its reply to the specific information requested.

104. The words "personal data concerning him or her" should not be interpreted in an "overly restrictive" way by controllers, as the Art. 29 Working Party already stated with regard to the right to data portability. Transposed to the right of access, the EDPB considers for example that recordings of telephone conversations (and their transcription) between the data subject that requests access and the controller, may fall under the right of access provided that the latter are personal data. [...]

150. It is the responsibility of the controller to decide upon the appropriate form in which the personal data will be provided. The controller can, although is not necessarily obliged to, provide the documents which contain personal data about

² Judgment of the Court of Justice of the European Union, Nowak, C-434/16, EU:C:2017:994, paragraphs 34-35.

³ Judgment of the Court of Justice of the European Union, Valsts, C-175/20, EU:C:2022:124, paragraphs 34 and 36.

the data subjects making the request, as such and in their original form. The controller can for example, on a case-by-case basis, provide access to a copy of medium given the need for transparency (for example, to verify the accuracy of the data held by the controller in the event of a request for access to the medical file or an audio recording whose transcript is disputed). However, the CJEU, in its interpretation of the right of access under the Directive 95/46/EC, stated that “for [the right of access] to be complied with, it is sufficient for the applicant to be provided with a full summary of those data in an intelligible form, that is, a form which allows him to become aware of those data and to check that they are accurate and processed in compliance with that directive, so that he may, where relevant, exercise the rights conferred on him”. Unlike the directive, the GDPR expressly contains an obligation to provide the data subject with a copy of the personal data undergoing processing. This, however, does not mean that the data subject always has the right to obtain a copy of the documents containing the personal data, but an unaltered copy of the personal data being processed in these documents. Such copy of the personal data could be provided through a compilation containing all personal data covered by the right of access as long as the compilation makes it possible for the data subject to be made aware and verify the lawfulness of the processing. Hence, there is no contradiction between the wording of the GDPR and the ruling by the CJEU regarding this matter. The word summary in the ruling should not be misinterpreted as meaning that the compilation would not encompass all data covered by the right of access, but is merely a way to present all that data without giving systematically access to the actual documents. Since the compilation needs to contain a copy of the personal data, it should be stressed that it cannot be made in a way that somehow alters or changes the content of the information.

EDPB Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, inter alia:⁴

3. In addition, connected vehicles are generating increasing amounts of data, most of which can be considered personal data since they will relate to drivers or passengers. Even if the data collected by a connected car are not directly linked to a name, but to technical aspects and features of the vehicle, it will concern the driver or the passengers of the car. As an illustration, data relating to the driving style or the distance covered, data relating to the wear and tear on vehicle parts, location data or data collected by cameras may concern driver behaviour as well as information about other people who could be inside or data subjects that pass by. Such technical data are produced by a natural person, and permit his/her direct or indirect identification, by the data controller or by another person. The vehicle can be considered as a terminal that can be used by different users. Therefore, as for a personal computer, this potential plurality of users does not affect the personal nature of the data

29. Much of the data that is generated by a connected vehicle relate to a natural person that is identified or identifiable and thus constitute personal data. For instance, data include directly identifiable data (e.g., the driver’s complete identity), as well as indirectly identifiable data such as the details of journeys made, the vehicle usage data (e.g., data relating to driving style or the distance covered), or the vehicle’s technical data (e.g., data relating to the wear and tear on vehicle

⁴ EDPB, Guidelines 01/2020 on processing staff data in the context of connected vehicles and mobility related applications, Version 2.0, adopted on 9 March 2021 following public consultation, paragraphs 3, 29 and 62; IMY translation

parts), which, by cross-referencing with other files and especially the vehicle identification number (VIN), can be related to a natural person. Personal data in connected vehicles can also include metadata, such as vehicle maintenance status. In other words, any data that can be associated with a natural person therefore fall into the scope of this document.

62. As noted in the introduction, most data associated with connected vehicles will be considered personal data to the extent that it is possible to link it to one or more identifiable individuals. This includes technical data concerning the vehicle's movements (e.g., speed, distance travelled) as well concerning the vehicle's condition (e.g., engine coolant temperature, engine RPM, tyre pressure). [...]

In the preparatory work documents for the law '*Road infrastructure charges and electronic toll systems*', the legislature⁵ noted that the very broad definition of personal data was the subject of discussion in the legislative file which resulted in the Law on road traffic registers⁶ and stated the following. In the field of road traffic there are both personal data and vehicle technical data. However, in some cases it may be difficult to determine to which category a particular task falls. A technical data of a vehicle should not be considered as personal data if it cannot be linked to the identity of the owner of the vehicle. On the other hand, an indication that a particular vehicle is subject to a driving ban refers to the owner of the vehicle in a specific way and it is therefore likely to be personal data. In the light of this statement, the Government considered in the preparatory work for the Act on⁷ Congestion Tax that the registration number of a vehicle also relates to the owner of the vehicle in such a specific way that the task is to be regarded as personal data. The Government does not consider that there is now any reason to make a different assessment.

In the literature, Öman states that vehicle registration numbers are examples of information relating to an identifiable natural person.⁸

Right of access without undue delay

The controller is obliged to provide any person who so requests with information on the processing or non-processing of personal data relating to the applicant. Processing such data shall, in accordance with Article 15 of the GDPR, provide the complainant with additional information as well as a copy of the personal data processed by the controller.

According to Article 12(3) GDPR, the controller shall upon request without undue delay and in any event no later than one month after receiving the request for access and respond to the data subject's request.⁹

Assessment of the Swedish Authority for Privacy Protection (IMY)

On the basis of the complaint in the case, IMY only examined the company's conduct in the individual case and whether it provided a copy of the personal data relating to

⁵ Prop. 2013/14:25 p. 85.

⁶ Prop. 2000/01:95 p. 98.

⁷ Prop. 2003/04:145 pp. 98 et seq.

⁸ Öman, S. Data Protection Regulation (GDPR) etc. 2, the commentary on Article 5, under the heading "*First paragraph — Personal data*".

⁹ European Data Protection Board Guidelines 01/2022 on data subjects' rights — right of access, version 1.0, adopted on 18 January 2022.

the complainant without undue delay. Supervision does not apply if the company's personal data processing is otherwise compatible with the General Data Protection Regulation (GDPR).

The IMY considers that the information requested by the complainant on technical records and data from the vehicle guarantee, constitute personal data relating to the applicant, since they relate specifically to the applicant as the owner of the vehicle and may be used to identify the complainant.¹⁰ In so doing, the complainant is entitled to access the data from the company upon request in accordance with Article 15 of the GDPR, inter alia, the information set out in Article 15(1) and a copy of the data pursuant to Article 15(3).

The complainant has stated that the request for access was made in March 2019. On the other hand, the company has states that the applicant's request for access was made only on 25 February 2020. IMY finds no reason to question the company's statements that the applicant's request was received by the company on 25 February 2020. However, IMY considers that this request was sufficiently clear and clear to refer to all personal data relating to the complainant's vehicles, including the above-mentioned data which the company made available to the applicant only on 15 September 2021. This is because the complainant indicated in its request the type of information about his vehicle for which the complainant requested data and that the controller should assume that, in the event of a request for access, the data subject intends to exercise his or her full right pursuant Article 15(1) to (2) of the GDPR.¹¹ The request has thus been met 17 months after the external deadline of one month for: to deal with the request in accordance with the general rule in Article 12(3). IMY therefore considers that Volvo Personvagnar AB has not dealt with the complainant's request for access pursuant Article 15(3) without undue delay within the meaning of Article 12(3) of the GDPR.

The fact that most of the information was disclosed earlier and that the company stated that the error was attributable to the human factor, does not cause any other assessment.

In the light of the above, IMY concludes that Volvo Personvagnar has processed the complainant's personal data in violation of Article 12(3) of the GDPR by not responding without undue delay to the complainant's request of 25 February 2020 for access pursuant Article 15(3) only on 15 September 2021.

Choice of corrective measure

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that the IMY has the power to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) provides which factors are to be taken into account when deciding on administrative fines and in determining the amount of the fine.

In the case of a minor infringement, as stated in recital 148, IMY may, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Factors to consider is

¹⁰ Cf. EDPB Opinion 01/2020 on Connected Vehicles, paragraphs 3, 29 and 62.

¹¹ Cf. EDPB Guidelines 01/2022 on data subjects' rights — right of access, version 1.0, adopted on 18 January 2022, paragraph 51.

the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and past relevant infringements.

IMY notes the following relevant facts. The infringement has affected one person and the company has reviewed its procedures. The company essentially satisfied the complainant's right of access without undue delay and has now also granted the complainant access to all his personal data. The Company has not received any corrective action for breach of GDPR. Against this background IMY considers that it is a minor infringement within the meaning of recital 148 and that Volvo Personvagnar AB must be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

This decision has been approved by the specially appointed decision-maker [REDACTED] after presentation by legal advisor [REDACTED]

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact information is shown in the first page of the decision.