Privacy Notice "Our Whistleblower System"

I. Scope of the privacy notice

In this privacy notice, we are informing you about the automated, electronic processing of your personal data by Volkswagen AG, Berliner Ring 2, 38440 Wolfsburg, Deutschland / Germany ("**we**", or "**VW**") in the context of our whistleblower system, for which we use several IT systems controlled by us.

The Whistleblowing System serves to receive and process hints about (presumed) legal or severe internal regulatory violations against the Volkswagen Group on a safe and confidential way.

II. Who is the controller for the processing?

The controller for the processing of your personal data is:

Volkswagen AG, Berliner Ring 2, 38440 Wolfsburg, Germany.

Tax identification number / Registration number: DE 115235681

Registered in the commercial register of the Braunschweig District Court under the number HRB 100484 ("Volkswagen AG"). Chairman of the Board: Oliver Blume.

In certain cases, reports are processed together with the respective group company (subsidiary) in order to ensure the independence of the audit, e.g. in the case of specific violations of the rules. For this purpose, personal data is also shared as part of joint controller processing. A corresponding joint controller agreement has been concluded for this purpose (Joint Controller Agreement, JCA) with the brand companies Audi AG, Porsche AG und TRATON. The subsidiaries affiliated with the brand companies pursuant to § 15 AktG have acceded to this agreement.

The JCA sets out the specific obligations, rights and responsibilities of the individual Group companies in the joint processing of personal data within the framework of the whistleblower system.

In the following, we inform you in accordance with Art. 26 (2) sentence 2 GDPR about the essential contents of this JCA.

For which stages of the process is there joint responsibility?

From a factual point of view, joint responsibility applies to serious regulatory violations. This applies in particular to the clarification of questions in the context of the preliminary check for plausibility of the hint and the conduct of the investigation in the event of a suspicion of a serious violation.

To this end, the Group companies rely on an uniform platform and uniform IT systems. The standardised procedure is intended to ensure that serious regulatory violations within the Volkswagen Group are investigated, remedied and, if necessary, punished independently and in accordance with uniform standards. The Group companies are each independently responsible for punishing and, if necessary, sanctioning serious regulatory violations by employees identified in the course of whistleblowing procedures. The associated data processing is covered by the JCA.

What does the JCA regulate?

The following section describes the main contents of the JCA.

Determination of data protection responsibility

In particular, the JCA specifies the responsibilities under data protection law within the framework of the whistleblower system. Volkswagen AG has a central role to play in the whistleblower system. The main

data protection responsibilities within the framework of the whistleblower system are presented below at a glance:

• Processes and structures: Volkswagen AG provides the technical and organizational infrastructure necessary for the effective implementation of whistleblowing procedures. This includes, among other things, the organization of internal and external reporting channels. Volkswagen AG is centrally responsible for the corresponding structures and processes.

• Data exchange with regard to incoming information: Group companies that receive information about possible serious regulatory violations are obliged to forward them centrally to Volkswagen AG.

• Handling of specific whistleblower proceedings – serious regulatory violations: If there are detailed indications of serious regulatory violations ("Serious regulatory violations" include, but are not limited to: criminal offences, violation of human rights, violation of US environmental regulations, obstruction of internal investigations, significant violation of basic ethnic values, impairment of the financial interests of Volkswagen AG) by employees, Volkswagen AG is responsible for carrying out the investigations to be initiated. whistleblower procedures. This applies, among other things, to the plausibility check of incoming information, the planning and implementation of necessary measures to clarify the facts and, if necessary, the preparation of a final report. The investigative measures may include, among other things, the questioning of implicated persons and the evaluation of data sets and documents.

• Handling of specific whistleblowing procedures – other regulatory violations: If there are detailed indications of other regulatory violations, the respective Group companies will carry out the whistleblowing procedures to be initiated independently (regulatory violations are intentional or negligent violations of applicable law (e.g. laws, ordinances, etc.) or internal company regulations, in particular violations of the Code of Conduct and regulatory violations of conduct contractual obligations by employees that they commit in connection with or on the occasion of their work for the Group company).

• Cooperation in the context of the investigation of the facts: Volkswagen AG and the Group companies involved, if any, will cooperate in whistleblower proceedings to ensure effective clarification of the suspicions communicated. This cooperation may require a mutual exchange of personal data.

• Data exchange after completion of the investigation of the facts: Volkswagen AG and the participating Group companies will exchange information with regard to the findings of the facts after the conclusion of the investigation of the facts and, if necessary, coordinate on the follow-up measures to be taken.

• Documentation of whistleblowing procedures: Volkswagen AG is centrally responsible for the documentation of whistleblowing procedures carried out.

• Information obligations: Volkswagen AG informs the implicated persons about the data processing that affects them in a general data protection information on the whistleblower system. Volkswagen AG or, if applicable, the Group company responsible for conducting a specific whistleblower procedure will also provide the data subjects with even more specific information on the processing of their personal data.

Further regulatory content

The JCA provides for further specific regulations for the protection of personal data within the framework of the whistleblower system. These regulations include in particular the following requirements:

• Requirements for data transfers (§ 1, No. 4 of the JCA);

• confidentiality obligations (§ 6 of the JCA);

• Technical and organizational data security measures to be taken by the Group companies (§ 11 of the JCA);

• Use of processors (§ 12 of the JCA);

• Mutual information obligations, for example in the context of data protection incidents or inquiries from data subjects (Section 9 of the JCA).

What does joint responsibility mean for data subjects?

The persons concerned can contact Volkswagen AG directly with inquiries using the contact details specified in Sections III and IV.

III. Who can I contact?

If you wish to assert your data protection rights, please use the contact options at

https://datenschutz.volkswagen.de/?lang=en-gb

There, you will find further information regarding how you can assert your data protection rights. You may also send your request

- via mail: Volkswagen AG, Privacy Team, Berliner Ring 2, 38440 Wolfsburg, Germany
- *via e-mail: privacy@volkswagen.de*
- *via telephone: 00800-8932836724889 (00800-VWDATENSCHUTZ)*

We take data subject rights very seriously and will respond to any request that you might have as soon as possible. If you have any general questions about this privacy notice or the processing of your personal data by Volkswagen AG, please use the following contact option:

io@volkswagen.de

IV. Contact details of the data protection officer

For matters concerning data protection, you can also consult our **company data protection officer**, using your own language:

Volkswagen Aktiengesellschaft

Mail Box 011/80910, 38436 Wolfsburg

E-Mail: dataprivacy@volkswagen.de

Dr. Oliver Draf

00800-8932836724889 (00800-VWDATENSCHUTZ)

V. Which rights do I have?

All the below named rights concerning the personal data and the processing thereof may be subject to limitations, according to the applicable EU and/ or national laws. Depending on your jurisdiction, as the data subject, you may be entitled to the following data protection rights. **Please note**: Your data protection rights under the local laws of the country where you are located at the relevant time may differ from the rights described below. Please see Annex 1 for additional, country-specific information, in particular on rights that you might have under local laws. Such rights apply, to the extent the legal requirements are met, in addition to your rights provided under the GDPR.

For more information about rights you may have in connection with our processing of your personal data, please click here:

https://datenschutz.volkswagen.de/?lang=en-gb

1. **Right to be informed**
2. **Right to access**
3. **Rectification**
4. **Erasure**
5. **Restriction of processing**
6. **Data portability**
7. **Objection**
8. **Withdrawal of consent**
9. **Complaint**

In addition, you have the right to lodge a complaint with a data protection supervisory authority if you believe that the processing of your personal data is unlawful. The right to lodge a complaint is without prejudice to any other administrative or judicial remedy. The address of the data protection supervisory authority responsible for VOLKSWAGEN is:

Der Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstraße 5
30159 Hannover
Deutschland / Germany

However, you can also lodge a complaint with any other data protection supervisory authority competent for you within or outside the EU, in particular with the one in the Member state of your habitual residence, place of work or place of the alleged infringement. Please find hereinafter a link where you can find all contact details of the national authorities in all member states: https://edpb.europa.eu/about-edpb/board/members_en.

See Appendix 1 "Additional rights of data subjects and further country-specific information" for contact details of national supervisory authorities and further country-specific information.

10. Information on your right to object

a) Right to object on grounds relating to your particular situation

You have the right to object to the processing of your personal data on grounds relating to your particular situation. The prerequisite for this is that the data processing takes place in the public interest or on the basis of legitimate interests. This also applies for any profiling. Insofar as we base the processing of your personal data on legitimate interests, we generally assume that compelling legitimate grounds can be demonstrated, but we will, of course, examine each individual case. In the event of an objection, we will no longer process your personal data, unless

- we can demonstrate compelling legitimate grounds for the processing of such data which override your interests, rights and freedoms or
- your personal data are used for the establishment, exercise or defence of legal claims or
- there are grounds permitting the processing of your personal data, notwithstanding your objection, under applicable local laws, provided that such processing is not restricted under the GDPR.

d) Exercise of the right to object

The objection can be exercised in any form and should preferably be addressed to the contact details listed in section III.

VI. Which data do we process for which purposes and which legal bases apply?

The whistleblower system is used to receive and process information about (suspected) violations of the law or serious internal rules against the Volkswagen Group in a secure and confidential manner.

The use of the whistleblower system is voluntary. We collect the following personal data and information when you submit a report:

• your name, if you disclose your identity,

• your contact details, if you provide them to us,

• the fact that you have made a report via the whistleblower system,

• whether you are employed by the Volkswagen Group, and

where applicable, names of individuals and other personal data of the individuals named in the notification. The personal data could include to the maximum extend:

- **Job-related contact and (work) organisation data** (e.g. Surname, given name, sex, address, email address, phone number, mobile phone number, (Group) company, area, department, cost centre, personnel number, responsibilities, functions, presence (yes/no), etc.)
- **IT usage data** (e.g. UserID, roles, permissions, log-in times, computer name, IP address, GID, Legic no., etc.)
- **Special category: Photo of the employee** (e.g. Portrait photo voluntarily published by the employee (intranet telephone directory, internal social media platform, etc.)
- **Private contact and identification data** (e.g. Surname, given name, sex, address, email address, phone number, mobile phone number, date / place of birth, identification numbers, nationality, etc.)
- **Contract data** (e.g. Purchased products, (financial) services, date of purchase agreement, purchase price, extras, warranties, etc.)
- **Vehicle usage data with VIN / number plate Guarantee, warranty, product liability, safe vehicle operation** (e.g. Data generated during vehicle use which is linked to the VIN / number plate and which is of importance in connection with workshop repairs, guarantees, warranties, product liability or the availability of what is required for the safe operation of the vehicle.)
- **Vehicle usage data with VIN / number plate Comfort settings, multimedia, navigation** (e.g. Data generated during vehicle use that are linked to the VIN / number plate and that relate to comfort settings, such as seat adjustment, preferred radio stations, climate settings, navigation data, email / SMS contact information, etc.)
- **Vehicle usage data with VIN / number plate Assistance systems, driving behaviour etc.** (e.g. Data generated during vehicle use that are linked to the VIN / number plate and that relate to the driving behaviour or the use of assistance systems and their specific operational data, etc.)
- **Position data** (e.g. GPS, wireless positioning / tracking, movement profile, WLAN hotspot tracking / positioning, etc.)
- **Data regarding personal / professional circumstances and characteristics** (e.g. Data concerning spouse or children, marital status, portrait photo, volunteer work, job title, career, length of service, tasks, activities, log-file analyses, joining and leaving dates, qualifications, assessments / evaluations, etc.)
- **Payment and time management data** (e.g. Pay scale group, payroll accounting, special payments, garnishment, daily attendance times, reasons for absence, etc.)
- **Creditworthiness and other financial data, bank details** (e.g. Payment behaviour, balance sheets, credit bureau data, credit score values, financial circumstances, bank account details, credit card number, etc.)
- **Special categories of personal data** (e.g. Special categories of personal data pursuant to Article 9(1) GDPR: racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation)
- **Criminal offences / regulatory offences** (e.g. Data relating to (suspected) criminal acts and other special requirements under Article 10 GDPR)

The whistleblower system uses certain AI functions from Microsoft Office 365 exclusively to support daily work processes (e.g. translations and text editing). There is no automated decision-making or profiling. It is ensured that Microsoft does not use the data entered in the whistleblowing system to improve or train its AI models.

Following on from the above, we process your personal data on the basis of the following legal bases for the following purposes:

1. Preliminary check & plausibility check: Volkswagen AG checks the responsibility for each hint case. Before initiating investigative measures, Volkswagen AG will examine, among other things, whether the information provided by the whistleblowers appears plausible and suggests a regulatory violation. Volkswagen AG will forward any information from whistleblowers that may also concern another Group company to them. The processing of your data also serves, among other things, to check whether a corresponding data transfer is necessary in individual cases.

2. Cooperation with ombudsman: You have the opportunity to submit hints to our external ombudsman. This is an external lawyer who is subject to legal confidentiality and assure the whistleblowers anonymity. The data processing carried out within the framework of the whistleblower system also serves, among other things, to cooperate with this ombudsman.

3. Investigation of misconduct: Investigative measures can serve, among other things, to uncover and clarify possible breaches of duty under the employment contract or criminal offences committed by employees in the performance of their official duties as well as other regulatory violations and grievances within the company. As part of the processing of reports or an investigation, it may be necessary to pass on information to other employees of Volkswagen AG or employees of the subsidiaries of Volkswagen AG, e.g. if the information relates to events in subsidiaries of Volkswagen AG. The processing is carried out under joint responsibility with the subsidiary.

4. Implementation of legal obligations: Volkswagen AG is subject to comprehensive statutory supervisory and compliance obligations. These result, among other things, from §§ 130, 30 of the Administrative Offences OWiG) and §§ 93, 111 of the Stock Corporation Act (AktG). Investigative measures serve to implement these and other legal obligations of Volkswagen AG. For example, we carry out investigative measures to ensure that our products comply with legal and regulatory requirements (product compliance) and to uncover possible conflicts of interest within the company.

5. Exercise of rights: Investigative measures can also serve to compensate for and avert imminent economic or other damage or disadvantages for Volkswagen AG and thus to effectively defend the law, exercise and enforce rights. For example, Volkswagen AG will use the results and information obtained through investigative measures in the context of labor court proceedings or other legal disputes, if necessary.

6. Implementation of obligations to cooperate: Volkswagen AG may be obliged to pass on the data collected in the course of the investigation measures to law enforcement authorities or other authorities on the basis of statutory obligations to cooperate. This may be the case, for example, if a prosecuting authority initiates criminal investigation proceedings against an implicated person as a result of an investigation measure. Volkswagen AG will only process your data to the extent that at least one applicable data protection regulation allows this. These include, in particular, the provisions of the GDPR, the BDSG and other relevant legal provisions.

Volkswagen AG may base permissible data processing in the context of investigation measures in particular on the following legal bases:

1. Establishment, implementation or termination of an employment relationship/employment contract (§ 26 (1) BDSG/Art. 6 (1b) GDPR),

2. Investigation of criminal offences (§ 26 (1) sentence 2 BDSG): If investigation measures serve to uncover possible criminal offences in the context of employment relationships, they may be justified under § 26 (1) sentence 2 BDSG.

3. Implementation of legal obligations (Art. 6 para. 1 lit. c GDPR) Volkswagen AG is subject to comprehensive statutory supervisory and compliance obligations. The investigative measures carried out by Volkswagen AG thus also serve, among other things, to implement these legal obligations of Volkswagen AG.

4. Works agreements (Art. 88 para. 1 GDPR, § 26 para. 4 BDSG): Volkswagen AG may also process your data on the basis of a valid works agreement that regulates the introduction and operation of the whistleblower system.

5. Safeguarding legitimate interests (Art. 6 para. 1 lit. f GDPR): Volkswagen AG may also process your data in order to protect its legitimate interests or those of a third party (does not apply to special categories of personal data and data from criminal offences / administrative offences). In individual cases, these legitimate interests may include:

• Legal defence: Volkswagen AG carries out investigative measures in order to avert damage to its own company, among other things. In this respect, data processing may also serve the legitimate interests of Volkswagen AG in the form of asserting, defending and exercising legal claims.

• Improvement of compliance structures: Investigative measures can also indirectly serve to improve Volkswagen AG's internal compliance structures.

• Support for implicated prsons: Investigative measures can also serve to relieve the burden on those affected, among other things. In principle, this is a legitimate interest of a third party.

• Implementation of foreign legal provisions: In addition to national and EU law requirements, Volkswagen AG is also subject to comprehensive compliance legislation from countries outside the EU. These include, for example, anti-corruption or competition guidelines under US law. In principle, ensuring compliance with such foreign legal provisions may also constitute a legitimate interest.

Volkswagen AG will ensure that investigative measures to safeguard legitimate interests are only carried out to the extent that there are no conflicting legitimate interests and rights of the implicated employees.

Please note: If the applicable local law of the country where you are located at the relevant time foresees additional requirements regarding the legal bases, we will comply with such additional requirements and will inform you accordingly.

VII. Who receives my data?

Within VOLKSWAGEN, those entities receive your data that they need to fulfil our contractual and statutory obligations and to safeguard our legitimate interests. Our service providers (so-called processors) that we utilise and engage may also receive data for these purposes. We will generally share your personal data with third parties only if this is necessary for the performance of the contract, if we or the third party have a legitimate interest in the disclosure, or if you have given your consent, subject to applicable local laws. In addition, data may be shared with third parties (including investigative or security authorities) to the extent we should be required to do so by law or by enforceable regulatory or judicial orders.

1. Processors

Service providers which are used and act on behalf of VOLKSWAGEN and that do not process data for any of their own purposes (so called "processors") may receive data for the purposes mentioned above. We utilise processors of the following categories for the provision of specific services, who support us in the execution of our business processes. Specifically, this includes:

Category of Processor	Name of Processor	Processing purpose

Technical Supplier	People Intouch B.V. Olympisch Stadion 6 1076 DE Amsterdam Netherlands	People Intouch provides the intake channels (Hotline, Webintake, App) through which Whistleblower reports are submitted to Volkswagen Group.

2. Is data transmitted to a third country?

As part of the processing of reports or an investigation, it may be necessary to pass on information to other employees of Volkswagen AG or employees of the subsidiaries of Volkswagen AG, e.g. if the information relates to events in subsidiaries of Volkswagen AG. The overview of the subsidiaries can be found below https://www.volkswagen-group.com/de/standorte-der-volkswagen-group-17481).

If necessary for the clarification, a transfer may be made to subsidiaries of the Volkswagen Group in a country outside the European Union or the European Economic Area, on the basis of suitable or appropriate data protection guarantees for the protection of implicated persons. Please note that not all third countries have an adequate level of data protection recognised by the European Commission. For data transfers to third countries in which there is no adequate level of data protection, we ensure that the recipient either has an adequate level of data protection (e.g. adequacy decision of the EU Commission or agreement of so-called EU standard contractual clauses of the European Union with the recipient) or that there is explicit consent from our users before the transfer. We always make sure that the relevant data protection regulations are complied with when passing on information. If there is a corresponding legal obligation or data protection law requirement for the clarification of information, law enforcement authorities, antitrust authorities, other administrative authorities, courts and international law firms and auditing firms commissioned by the Volkswagen Group may be considered as other conceivable categories of recipients. Any person who gains access to the data is bound by a duty of confidentiality.

VIII. How long will my data be stored?

We store your data as long as necessary for the provision of our services to you or do so if we have a legitimate interest in the continued storage.

We will store your data for the duration of the relevant statutory storage obligations (generally up to 3 years). In addition, the storage period in case of potential violations against supply chain due diligence act is up to 7 years.

In addition, we are subject to various retention and documentation obligations, which result, inter alia, from the German Commercial Code (*Handelsgesetzbuch,* "**HGB**") and the German Tax Code (*Abgabenordnung,* "**AO**"). The periods specified therein for retention and documentation are up to ten years. Finally, the storage period is also assessed according to the statutory limitation periods, which can be up to thirty years, for example, according to §§ 195 et seqq. of the German Civil Code (*Bürgerliches Gesetzbuch*, "**BGB**"), with the regular period of limitation being three years.

Under certain circumstances, your data may also need to be retained for a longer period of time, such as when a so-called legal hold or litigation hold (i.e. a prohibition of data deletion for the duration of the proceedings) is ordered in connection with administrative or judicial proceedings.

We may also be subject to retention and documentation obligations in line with the local legislation of your country.

IX. Is there an obligation for me to provide data or to give consent?

In the context of the whistleblowing system, you need to provide only the personal data you want or that we are required or permitted to collect by law. You can give an anonyminous hint. However, without complete and accurate data, VOLKSWAGEN may not be able to contact you and investigate a potential misconduct. If we are asking you for your consent to the processing of your personal data, such consent will always be voluntary. However, if you do not give your consent, we might not be able to provide a particular service, if the relevant service cannot be provided without such data.

X. What practices and procedures are implemented to secure my data?

We have implemented and maintain at all times encompassing technical and organisational measures (***TOMs***) to protect your data in accordance with the high standards of the GDPR and the standards required under other applicable local laws of the jurisdiction you may be located at. This includes, but is not limited to, pseudomysation and encryption, measures to ensure the ongoing confidentiality, integrity and availability of your data (including the ability to restore data in case of an incident). We are regularly reviewing our TOMs and apply enhancements where needed to keep your data safe and to comply with applicable laws. We have put in place appropriate procedures to deal with any personal data breach (i.e. a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed) and will notify you as the data subject and relevant supervisory authority when we are legally required to do so.

XI. Updates of this privacy notice

We might update this privacy notice from time to time by making available updates to this privacy notice on our website.

Version: 02.05.2025

Annex 1 – Additional data subject rights and further country-specific information

Argentina

You have the right to

- access;
- rectification;
- erasure;
- file a complaint regarding the processing of your personal data to THE PUBLIC INFORMATION ACCESS AGENCY, which, depending on the facts of the individual case, in its capacity as the Control Entity of Law No. 25,326, has the power to attend complaints and claims filed by those whose rights are affected due to breaches with applicable regulations on personal data protection.

Australia

You have the right to

- access;
- rectification;
- lodge a complaint with both VOLKSWAGEN and the Office of the Australian Information Commissioner ("OAIC") or any other dispute recognition scheme recognised by the OAIC which can be found on the OAIC website www.oaic.gov.au.

  If you are concerned with the way we have handled your personal data, you may lodge a privacy complaint with the Office of the Australian Information Commissioner ("OAIC"). However, it is a requirement of the OAIC that prior to lodging a complaint, you have raised your complaint with us. If you are not satisfied with our response or we fail to provide a response within 30 days of receipt, you can lodge a complaint with the OAIC. The contact details for the OAIC are set out below:

Phone	1300 363 992
Fax	(02) 9284 9666
Website	https://www.oaic.gov.au/
Post	GPO Box 5288, Sydney NSW 2001

Brazil

You have the right to

- to be informed about the collection and use of your personal data, by us, in a readily accessible manner, and in plain and clear language. You also have the right to be informed about any public or private entity with whom your data has eventually been shared. We are implementing your right to be informed, also through this notice, the content of which may be updated from time to time.
- information access;
- obtain a copy when the legal basis for processing is consent or performance of a contract;
- erasure when consent is the legal basis for processing: please note that exceptions to this right might apply, namely, when the data is needed for (i) compliance with legal obligations; (ii) study

by a research organization; (iii) transfer to third parties; (iv) use solely by the controller, as long as the data is anonymized;

- rectification;
- object to the processing (e.g. if the data is being unlawfully processed);
- data portability;
- withdraw consent at any time;
- anonymize, block or delete unnecessary or excessive personal data or data processed in non-compliance with data protection law;
- review decisions made solely on the basis of automated processing;
- lodge a complaint before ANPD (Autoridade Nacional de Proteção de Dados) against the data controller;
- be informed of the possibility of not providing consent and the consequences thereof;
- be informed about the public and private entities with whom the data has been shared.

Colombia

Data Subject's Rights

Pursuant to the provisions of art. 8 of Law 1581 of 2012, you have the right to

- know, update and rectify your Personal Data from the Controller or the Processor. This right can be exercised, among other, regarding partial data as well as in respect to data that is incomplete or fractioned, that induces error, or those whose Processing is expressly forbidden or has not been authorized;
- request evidence of the authorization granted to the Controller unless when it is expressly excepted as a requirement for the Processing, pursuant to the provisions of article 10 of law 1581 of 2012;
- be informed by the Controller or the Processor upon request, in respect to the use that has been made of your Personal Data;
- file to the Superintendence of Industry and Commerce complaints for infractions to the provisions of Law 1581 of 2012 as amended, added to or supplemented from time to time;
- revoke the authorization and/or to request the deletion of the specific data, provided that there is no legal or contractual obligation that imposes on you the duty to remain in the database;
- have access, free of charge, to your Personal Data that has been the subject of Processing, at least once per calendar month and whenever there are substantial amendments to the Processing policies.

Procedures you have to follow to exercise your personal data rights

A. Complaints: You may file complaints regarding the Personal Data kept in VOLKSWAGEN's databases, according to the following rules:
    - The complaint will be analyzed to verify your identification. If the complaint is made by a person other than you and the capacity of such person is not accredited according to the laws in force, the complaint will be rejected.
    - All the complaints will be resolved in a maximum term of ten (10) business days as from the date in which the same are received. If it is not possible to answer the complaint within said term, you will be informed, expressing the reasons for the delay and informing a date

in which the enquiry will be answered, which cannot exceed, in any case, five (5) business days after the expiration of the original term.

B. Requests: If you consider that the data contained in VOLKSWAGEN's databases must be subject to corrections, updates or deletion, or when they notice the alleged breach of any of the duties, you may file a request according to the following rules:

- The requests will be analyzed to verify your identification. If the request is made by a person other than you and the representation thereof is not accredited according to the regulations in force, the request will be rejected.
- The request must contain the following information: (i) your identification; (ii) contact data (physical and/or electronic address and contact phone numbers); (iii) the documents that accredit your identity, or your representation; (iv) The clear and precise description of the Personal Data regarding which you seek to exercise any of the rights; (v) The description of the facts that lead to the request; (vi) The documents that they intend to enforce; (vii) signature and identification number.
- If the request is incomplete, VOLKSWAGEN shall make a requirement to you, within a term of five (5) days after the receipt of the request, to remedy the defects. If two (2) months lapse from the date of the requirement and you have not given the information required, it shall be construed that you have desisted the request.
- If the area that receives the request is not competent to answer it, it shall pass it to the relevant area or person within a term of two (2) business days and will inform this situation to the interested party.
- Once the complete request has been received, a note saying "request being processed" shall be included in the database with the reason thereof, in a term of no more than two (2) business days. Said note must be left in place until the moment in which the claim is decided.
- The maximum term to answer the request will be fifteen (15) business days as from the day after the date in which it is received. When it is not possible to answer the request within that term, the reasons of the delay shall be informed to the interested party together with the date in which the request will be answered, which under no circumstances can exceed eight (8) business days after the expiration of the first term.
- You have the right, at all times, to request the deletion of you Personal Data. The deletion implies the total or partial removal of the Personal Data from the Data Bases, according to your request. The deletion right is not absolute and VOLKSWAGEN may refuse the exercise thereof in the following events: (i) If you have a legal or contractual duty to remain in the Database or if the Controller has a legal or contractual obligation that means that it has to keep the Personal Data; (ii) The deletion of the Personal Data would thwart judicial or administrative activities related to fiscal obligations, the investigation and persecution of crimes or the update of administrative sanctions; (iii) The Personal Data is necessary to protect your interests protected by the laws, to perform an action pursuant to the public interest, or to comply with an obligation legally acquired by you or by the Controller.

Authorization: As from the enactment of this notice, at the time of the collection of Personal Data, VOLKSWAGEN shall request the prior authorization from you and you shall be duly informed about the specific purposes of the Processing for which such consent has been obtained, excepting in the case of any one of the exceptions provided in article 10 of Law 1581 of 2012 for such purposes.

VOLKSWAGEN may transmit and/or transfer your Personal Data to third parties located in Colombia or abroad, as long as VOLKSWAGEN has the prior and express authorization of you of the Personal Data.

Retention period: The information provided by you shall only be used for the purposes herein established. Once the need for the Processing of the Personal Data has ceased, the same shall be deleted from VOLKSWAGEN's databases.

Hong Kong

In addition to your rights set out in Sec. V you may withdraw your consent to the use of your personal data.

India

You have the right to

- access (i.e., the right to be informed if and to which extent we process your data);
- rectification (i.e., the right to have corrected false or incorrect data);
- withdraw consent;
- nominate (this right allows individuals to choose another person who can act on their behalf and exercise their rights under the DPDP Act in case they are unable to do so themselves due to death or incapacity);
- contact the Grievance Officer. The Data Protection Officer is the Grievance Officer for VOLKSWAGEN AG. For the contact details please see Sec. III.

You can assert your rights at any time by usind the contact details set out in Sec. III.

Israel

You have the right, subject to Protection of Privacy Law, 5741-1981 and the regulations enacted therefrom, to

- be informed if you are under a legal duty to provide the data, the purpose of collection, and details of any third party that will receive the data and for what purpose;
- access;
- rectification: request correction of the inaccurate or missing data or request deletion or destruction of the data;
- object to the processing (e.g. if the data is being unlawfully processed).

Japan

You have the right to

- request information on purpose of use;
- request information on security control measures;
- request access;
- request correction, addition or deletion;
- request discontinuance of use or erasure; and
- request explanations on data processing.

You also have the right to lodge a complaint with the Japanese authority, PPC as below:

Personal Information Protection Commission, Government of Japan (PPC),

Kasumigaseki Common Gate West Tower 32nd Floor, 3-2-1, Kasumigaseki, Chiyoda-ku, Tokyo, 100-0013, Japan

TEL: +81-3-6457-9680

Malaysia

You have the right to

- request access to your personal data;
- request correction of your personal data;
- prevent processing likely to cause damage or distress; and
- prevent processing for purposes of direct marketing.

Upon exercising your rights stated above in written form addressed to the contact details listed in section B. II., if you are dissatisfied with our response or we fail to provide a response within 21 days of receipt, you have the right to submit an application to the Personal Data Commissioner to require us to comply with your request. The application to the Personal Data Commissioner can be made to the following address:

Commissioner of Personal Data Protection, 6 th Floor, KKMM Complex Lot 4G9, Persiaran Perdana, Presint 4 Federal Government Administrative Centre 62100 Putrajaya.

In the event of any inconsistencies between the English version and the Bahasa Malaysia version of this privacy notice, the English version shall prevail.

Mexico

You have the right to:

- access;
- rectify;
- cancel;
- oppose;
- file data protection measures with the Federal Institute for Access to Information and Data Protection;
- request a reconsideration of a decision made via automated decision making in case you are of the opinion that the data processed in this context is (partly) incomplete or incorrect.

Please note the processing for the purposes set out above in Sec. VI includes the sensitive data you may provide us with your hint. Sensitive data is defined as *"the personal data that affects the most intimate sphere of its holder, or whose improper use may give rise to discrimination or entail serious risk for the holder. In particular, sensitive data are considered those that may reveal aspects such as racial or ethnic origin, present and future state of health, genetic information, religious, philosophical and moral beliefs, union membership, political opinions, sexual preference.".*

New Zealand

You have the right to

- know what personal data is held;
- request for personal data held and access the personal data;
- rectification;

- a response to your request within 20 working days, if you make a request for access to or rectification of your personal information. In limited circumstances, VOLKSWAGEN may extend this 20 working day time limit, but we must tell you the period of the extension and the reasons for the extension.
- lodge a complaint with both VOLKSWAGEN and the Privacy Commissioner. However, it is a requirement that before you can complain to the Privacy Commissioner you must first raise your complaint with VOLKSWAGEN. If you are not satisfied with VOLKSWAGEN's response or you do not receive a response, you can lodge a complaint to the Privacy Commissioner. In general, you should wait at least 30 working days for a response before contacting the Privacy Commissioner to lodge a complaint.

North Macedonia

You have the right to also contact the authorized representative for Volkswagen AG in the Republic of North Macedonia in case of any query related to the processing of your data and your data subject rights:

Porsche Macedonia DOOEL, Skopje
Blvd. Bosnia and Herzegovina 4
1000 Skopje
North Macedonia
Email: dataprivacy@volkswagen.de

Serbia

You have the right to be informed about appropriate safeguards in case of a data transfer to countries or international organisations outside Serbia that do not provide an adequate level of data protection recognised by a Serbian Government Decision. All EU / EEA Member states provide an adequate level of data protection recognised by a Serbian Government Decision.

Singapore

You have statutory rights as provided under Singapore's Personal Data Protection Act 2012, including the rights to

- request access to your personal data;
- request correction of your personal data; and
- withdraw consent to the collection, use or disclosure of your personal data (where applicable), subject to any grounds for the collection, use or disclosure without your consent that are required or authorised under the Personal Data Protection Act 2012 or any other written law of Singapore.

South Africa

You have the right to

- not have your personal data processed for the purposes of direct marketing by unsolicited electronic communication;
- initiate civil proceedings;
- be informed if your personal information has been compromised;

- be informed, free of charge and before the information is included in a directory, should you be a subscriber to a printed or electronic directory;
- lodge a complaint to the Information Regulator of South Africa by completing this form (https://inforegulator.org.za/wp-content/uploads/2020/07/FORM-5-COMPLAINT-REGARDING-INTERFERENCE-WITH-THE-PROTECTION-OF-AN-ADJUDICATOR.pdf) and sending it to POPIAComplaints@inforegulator.org.za.

For further information about your South African data privacy rights, please click here which will take you to the website of the Information Regulator.

South Korea

You (and your legal representative) have statutory rights under the Korean Personal Information Protection Act, in particular the right to

- access;
- rectification / erasure;
- suspension of processing; and
- withdrawal of consent.

You (or your legal representative) can exercise such rights by contacting us or our data protection officer using the contact details set out in Section III.

Certain personal data may be retained for compliance with local laws and regulations for certain periods, such as the following:

- All transaction records and relevant documentary evidence as prescribed by applicable tax laws: 5 years (as required under the Framework Act on National Taxes and the Corporate Tax Act)
- Records of logins: 3 months (as required under the Protection of Communications Secrets Act)
- Records on labels and advertisements: 6 months (as required under the Act on Consumer Protection in Electronic Commerce)
- Records on revocation of contracts or cancellation of orders/purchases, payments, provision of products and services: 5 years (as required under the Act on Consumer Protection in Electronic Commerce)
- Records on handling of customer complaints or disputes: 3 years (as required under the Act on Consumer Protection in Electronic Commerce

The process and method for destroying personal data are set forth below.

- Process of destruction: We select the relevant personal data to be destroyed and destroy it with the approval of our Data Protection Officer.
- Method of destruction: We destroy personal data recorded and stored in the form of electronic files by using a technical method (e.g., low level format) to ensure that the records cannot be reproduced, while personal data recorded and stored in the form of paper documents shall be shredded or incinerated

If it is necessary to retain personal data for a period longer than the legal retention periods described herein, to the extent required by the laws of the applicable country, we shall obtain the data subject's consent for such longer retention of personal data.

Taiwan

You have the right to

- make an inquiry of and to review your personal data;
- request a copy of your personal data;
- supplement or correct your personal data;
- demand the cessation of the collection, processing or use of your personal data; and
- erase your personal data.

Thailand

Please note that your right to obtain a copy of the personal data is subject to law or pursuant to a court order, and must not adversely affect the rights and freedoms of others.

Turkey

You have statutory rights under Art. 11 of the Turkish Data Protection Law, in particular the right to

- request reporting of the operations carried out which are rectification of the incomplete or inaccurate data, if any and the erasure or destruction of your personal data) to third parties to whom your personal data have been transferred;
- claim compensation for the damage arising from the unlawful processing of your personal data;
- object to the occurrence of a result against yourself by analyzing the data processed solely through automated systems,
- lodge a complaint with the Turkish Data Protection Authority (Kişisel Verileri Koruma Kurumu) Nasuh Akar Mahallesi 1407. Sok. No:4, 06520 Çankaya/Ankara/Turkey.

The objection can be exercised in the forms stated in Article 5/1 of the Comminuque On The Principles and Procedures for the Request To Data Controller.

You have the right to also contact the Data controllers representative in case of any query related to the processing of your data and your data subject rights:

Hergüner Bilgen Üçer Attorney Partnership
Büyükdere Caddesi 199
Levent 34394
Istanbul - TURKEY

(+90) 212 310 18 00

info@herguner.av.tr