At Valeo we are serious about preventing issues, managing risks and reducing our exposure to non-compliance with laws and regulations. We encourage our internal and external stakeholders to help us prevent and detect issues by speaking up when they witness or suspect an activity in violation of our Ethics & Compliance Programs or the laws according to the Valeo Whistleblowing Procedure.

The Valeo Whistleblowing System we have put in place offers whistleblowers various avenues to place an alert. Any alert and subsequent investigations entailed the collection and processing of personal data.

Personal Data Protection is important to us, and so is being transparent about how we collect, use, and share information. This Privacy Notice is intended to help you understand, in relation to our Whistleblowing System and procedures:

1. What information do we collect?
2. What do we use Personal Data for?
3. How do we collect personal data
4. Who receive your Personal Data?
5. How long do we store your Personal Data
6. What legal basis do we have for processing your Personal Data?
7. How do we secure Personal Data?
8. Your rights in relation to Personal Data
9. How to contact us?
10. Updating of the Privacy notice

For personal information that we generally collect when you interact with Valeo, please consult our privacy notice on valeo.com. If you are a Valeo employee, please consult our Employee Data Protection policy for how we process your data for general employment purposes.

1. What information do we collect?

We collect and process information necessary to process Alerts and properly investigate the facts that are being reported through the Whistleblowing System. The handling and investigating of an Alert may include the collection and processing of Personal Information, including but not limited to, the following categories:

- **Information concerning the Whistleblower:** first and last name, address, office location, telephone number, email address, job title, rank, internal identification number, picture, traffic data.
- **Information concerning the Person reported or suspected:** first and last name, address, office location, telephone number, email address, job title, rank, internal identification number, picture, traffic data.
- **Information concerning the facts being reported:** description of the facts whatever the media (e.g. mail, document, slides, reporting, picture, etc), date, location, individual(s) involved, legal issues, pieces of evidence, witnesses, testimonies.
- **Information concerning the individual(s) involved in the handling and investigation of the Alerts:** first and last name, address, office location, telephone number, email address, job title, rank, internal identification number.
2. **What do we use Personal Data for?**

Personal data may be used to:
- process Alerts;
- conduct investigations;
- determine what actions may be required (such as disciplinary, judicial actions, programs improvement, etc);
- compile and present statistics to the Alert Committee such as the number of alerts we receive but in an anonymous form.

3. **How do we collect personal data**

The personal information that we collect about you broadly falls into the following categories:
- Information that you provide voluntarily either by responding to the Whistleblowing System questionnaire or during the course of the investigation in response to the investigation team’s questions or requests for clarification/precision.

Except in India where it is prohibited by law, whistleblowers may choose to identify themselves or remain anonymous. While alerts can be anonymous, whistleblowers are generally advised by data protection authorities to identify themselves when submitting reports through a Whistleblowing System.

- Information that we obtain from third party sources about you and any individuals mentioned in your alert from third party sources (including internal records) in relation to the investigation.

4. **Who receives your Personal Data?**

We treat Alerts in strict confidence and ensure communications are on a need-to-know basis to those with a legitimate, business need. Subject to the above conditions and, where required, the signature of an NDA, your personal information are only disclose to:
- the two Designated Contacts appointed by the Group to receive, analyse and process the Alerts that are submitted through the Whistleblowing System.
- our Europe based third party provider, Got Ethics Ltd and, where necessary with Com Text A/S, who help manage the Alert System. We have strict contractual controls in place with Got Ethics Ltd, who must follow our instructions regarding your personal information. Using an external provider ensures confidentiality to anyone filing a report, and anonymity to those who choose to remain anonymous.
- the Investigation team;
- the Alert Committee;
- the Audit & Risk Committee;
- any competent law enforcement body, regulatory, government agency, court or our legal advisors where we believe disclosure is necessary (i) as a matter of applicable law or regulation, (ii) to exercise, establish or defend our legal rights, or (iii) to protect your vital interests or those of any other person;
- any Persons of knowledge who may have information that would help to understand the facts being reported.

The above recipient may be located in countries other than the country in which you are resident. These countries may have data protection laws that are different to the laws of your country.
However, we have taken appropriate safeguards to require that your personal data will remain protected in accordance with this Privacy Notice. These include implementing the Valeo Data Protection General & Specific Principles (VDPP) and require all parties to protect personal information they process from the EEA in accordance with European Union data protection law.

5. How long do we store your Personal Data

We retain personal information we collect where we have an ongoing legitimate business need to do so (for example, to deal with an Alert or to comply with applicable legal requirements).

When we have no ongoing legitimate business need to process personal data, we will either delete or anonymize it or, if this is not possible (for example, because personal data has been stored in backup archives), then we will securely store personal data and isolate it from any further processing until deletion is possible.

6. What legal basis do we have for processing your Personal Data?

We will collect personal information for the Whistleblowing System (i) where we are under a legal obligation to offer a whistleblowing service, or (ii) where the processing is in our legitimate interests to investigate Alerts and not overridden by the Data Subjects’ rights and freedoms.

7. How do we secure Personal Data?

We use appropriate technical and organizational measures to protect the personal information that we collect and process about you. The measures we use are designed to provide a level of security appropriate to the risk of processing your personal information.

The Alerts, investigation reports, presentations to the Alert Committee, recommendations, action plans and conclusions are recorded on a secure Drive.

Access to the Drive is subject to allocation of access rights by the responsible Designated Contact or the Chief Fraud Investigator. This access right is personal, confidential and targeted, i.e. it only gives access to certain specific information.

Access rights are rechecked monthly and information is archived in accordance with the Whistleblowing Procedure, using AES-256 encryption, so that the information is not accessible on-line.

8. Your rights in relation to Personal Data

Depending on where you use the Whistleblowing System from, you have the below data protection rights. You can exercise them by contacting us using the contact details provided under the “How to contact us” heading below:

► If you wish to access, correct, update or request deletion of your personal data.

► In addition, you can object to processing of your personal data, ask us to restrict processing of your personal data or request portability of your personal data.

► Similarly, if we have collected and process your personal data with your consent, then you can withdraw your consent at any time. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal information conducted in reliance on lawful processing grounds other than consent.

► You have the right to complain to us using the contact details provided below or to your data protection authority about our collection and use of your personal data.
We respond to all requests we receive from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws.

9. How to contact us?

Should you have questions or concerns about data protection, your personal data, or should you wish to file a complaint, please contact the Valeo Data Protection Officer at:

- dpo.internal@valeo.com for Valeo employees
- dpo.external@valeo.com for external stakeholders

10. Updating of the Privacy Notice

We may update this Privacy Notice periodically and without prior notice to reflect legal or technical changes or changes in Valeo’s internal procedures or data protection practices. Updated versions will be available on valeo.com and on the Ethics & Compliance Portal (employees only).