Exide Technologies S.A.

(“we”, “us”, “Company”)

Data Protection Policy (“Policy”)

The person (“you”, “your” or “user”) using the website to send personal information (“personal data”) is required to read this policy because it provides important information about:

- the data protection principles with which we must comply;
- what constitutes personal data and sensitive personal data;
- how we collect, use and (ultimately) delete personal data and sensitive personal data in accordance with the Policy;
- where more detailed information regarding the data can be found, e.g., the personal data we gather and use, how the personal data is used, stored and transferred, for what purposes, the steps taken to keep that personal data secure and for how long it is kept;
- your obligations as user or the website in relation to data protection; and
- the consequences of failure to comply with this Policy.

1 Introduction

1.1 By using the website we may obtain, keep and use your personal data for a number of specific lawful purposes.

1.2 The Policy sets out how we comply with our data protection obligations. The purpose of the Policy is also to ensure that users understand and comply with the rules governing the collection, process and deletion of personal data to which the Company and its employees may have access in the course of the relationship with you.

1.3 The Company is committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal data, and how (and when) we delete that information once it is no longer required.

1.4 If you have any questions or comments about the content of the Policy or if you need further information, you should contact the local Data Protection Offices or the Legal Department.

2 Scope

2.1 Users should refer to our other relevant policies, including the ones about information security and record retention, which contain further information regarding the protection of personal data in those contexts.

2.2 The Company commits to review and update the Policy in accordance with our data protection obligations periodically. The Policy does not form part of any employee’s contract of employment and we may amend, update or supplement the Policy from time to time. We will publish any new or modified policy in the website when it is adopted.

3 Definitions

criminal records information	means personal data relating to criminal convictions and offences, allegations, proceedings, and related security measures;
data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data;
data subject	means the individual to whom the personal data relates;
personal data	means information relating to a data subject who can be identified (directly or indirectly) from that information;
processing data	means collecting, obtaining, recording, organizing, storing, amending, retrieving, disclosing and/or destroying personal data, or more generally using or doing anything with it;
Pseudonymized	means the process by which personal data is processed in such a way that it cannot be used to identify a data subject without the use of additional information, which is kept separately and subject to technical and organizational measures to ensure that the personal data cannot be attributed to an identifiable data subject;
sensitive personal data	means special categories of personal data about a data subject's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify a data subject) and information concerning a data subject's health, sex life or sexual orientation.

4 Data protection principles

4.1 We will comply with the following data protection principles when processing personal data:

4.1.1 we will process personal data lawfully, fairly and in a transparent manner;

4.1.2 we will collect personal data for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

4.1.3 we will only process the personal data that is adequate, relevant and necessary for the relevant purposes;

4.1.4 we will keep accurate and up to date personal data, and take reasonable steps to ensure that inaccurate personal data are deleted or corrected without delay;

4.1.5 we will keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed; and

4.1.6 we will take appropriate technical and organizational measures to ensure that personal data are kept secure and protected against unauthorized or unlawful processing, and against accidental loss, destruction or damage.

5 Basis for processing personal data

5.1 In relation to any processing activity, the Company will, before the processing starts for the first time and then regularly while it continues:

5.1.1 review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:

(a) that the data subject has consented to the processing;

(b) that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) that the processing is necessary for compliance with a legal obligation to which the Company is subject;

(d) that the processing is necessary for the protection of the vital interests of the data subject or another natural person; or

(e) that the processing is necessary for our legitimate interests or those of a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject (see clause 5.2 below).

5.1.2 except where the processing is based on consent, satisfy us that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);

5.1.3 document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;

5.1.4 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy policies;

5.1.5 where sensitive personal data is processed, also identify a lawful special condition for processing that information (see paragraph 6.2.2 below), and document it; and

5.1.6 where criminal record is processed in accordance to Union or Member State law, also identify a lawful condition for processing that information, and document it.

5.2 When determining whether the Company's legitimate interests are the most appropriate basis for lawful processing, we will:

5.2.1 conduct an appropriate legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify our decision;

5.2.2 if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA); and,

5.2.3 include information about our legitimate interests in our relevant privacy policies.

6 Sensitive personal data

6.1 Sensitive personal data is referred to special categories of personal data.

6.2 The Company may from time to time need to process sensitive personal data. We will only process sensitive personal data if:

6.2.1 we have a lawful basis for doing so as set out in paragraph 5.1.1 above, e.g., it is necessary for the performance of an employment contract, to comply with Exide's legal obligations or for the Company's legitimate interests; and

6.2.2 one of the special conditions for processing sensitive personal data applies, e.g.:

(a) the data subject has given explicit consent;

(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of Exide or the data subject;

(c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

(d) processing relates to personal data which are manifestly made public by the data subject;

(e) the processing is necessary for the establishment, exercise or defense of legal claims; or

(f) the processing is necessary for reasons of substantial public interest.

6.3 Sensitive personal data will not be processed by us until:

6.3.1 the data subject has been properly informed (by way of the Policy or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

6.4 The Company will not carry out automated decision-making (including profiling) based on any data subject's sensitive personal data.

6.5 The Company will set out, when required, the types of sensitive personal data that will process, what it is used for and the lawful basis for the processing.

6.6 In relation to sensitive personal data, the Company will comply with the procedures technical and legally necessary to make sure that it complies with the data protection law and principles.

7 Criminal records information

As a fundamental and general principle, any criminal records information will be processed by the Company as it is not necessary for the purposes of this website. Notwithstanding, in the case we are compelled to do so by any legal obligations, we commit to do it in accordance and strict compliance with the Union or Member State law.

8 Data protection impact assessments (DPIAs)

8.1 Where processing is likely to result in a high risk to a data subject's data protection rights (e.g., where the Company plans to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

8.1.1 whether the processing is necessary and proportionate in relation to its purpose;

8.1.2 the risks to data subjects; and

8.1.3 what measures can be put in place to address those risks and protect personal data.

8.2 Before any new form of technology is introduced, the manager responsible should therefore contact the Data Protection Offices in order that a DPIA can be carried out.

8.3 During the course of any DPIA, the Company will seek the advice and the views of any other relevant stakeholders.

9 Documentation and records

9.1 We will keep written records of processing activities, including:

9.1.1 the name and details of the Exide legal entity (and where applicable, of other controllers);

9.1.2 the purposes of the processing;

9.1.3 a description of the categories of data subjects and categories of personal data;

9.1.4 categories of recipients of personal data;

9.1.5 where relevant, details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;

9.1.6 where possible, retention schedules; and

9.1.7 where possible, a description of technical and organizational security measures.

9.2 As part of our record of processing activities we document, or link to documentation, on:

9.2.1 information required for privacy policies;

9.2.2 records of consent;

9.2.3 controller-processor contracts;

9.2.4 the location of personal data;

9.2.5 DPIAs; and

9.2.6 records of data breaches.

9.3 If we process sensitive personal data or criminal records information, we will keep written records of:

9.3.1 the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;

9.3.2 the lawful basis for our processing; and

9.3.3 whether we retain and erase the personal data in accordance with the Policy and, if not, the reasons for not following the Policy.

9.4 We will conduct regular reviews of the personal data we process and update our documentation accordingly.

10 Data subjects' rights

10.1 Data subjects have the following rights in relation to their personal data:

10.1.1 to be informed about how, why and on what basis that data is processed;

10.1.2 to obtain confirmation that their data is being processed and to obtain access to it and certain other information, by making a subject access request;

10.1.3 to have data corrected if it is inaccurate or incomplete;

10.1.4 to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing;

10.1.5 to restrict the processing of personal data where the accuracy of the information is contested, or the processing is unlawful; and

10.1.6 to restrict the processing of personal data temporarily where they do not think it is accurate, or where they have objected to the processing;

11 Data subjects' obligations

11.1 Users are responsible for helping us keep their personal data up to date.

11.2 You should contact us if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

11.2.1 processing of personal data without a lawful basis for its processing;

11.2.2 any data breach;

11.2.3 any unauthorized access to personal data;

11.2.4 personal data not kept or deleted securely;

11.2.5 removal of personal data from the Company's premises without appropriate security measures being in place;

11.2.6 any other breach of the Policy or of any of the data protection principles.

12 Data subject access

12.1 Data subjects may make a request ("SAR") at any time to find out more about the personal data which the Company holds about them. The Company is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

12.2 All subject access requests received must be forwarded to the local Data Protection Officer.

12.3 The Company does not charge a fee for the handling of normal SARs. We reserve the right to charge reasonable fees for additional copies of information that have already been supplied to a data subject, or for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

13 Information security

13.1 The Company will use appropriate technical and organizational measures to keep personal data secured, and in particular to protect against unauthorized or unlawful processing and against accidental loss, destruction or damage. These may include:

13.1.1 making sure that, where possible, personal data is pseudonymized or encrypted;

13.1.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

13.1.3 ensuring that, in the event of a physical or technical incident, availability and access to personal data can be restored in a timely manner; and

13.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

13.2 Where the Company uses external organizations to process personal data on its behalf, additional security arrangements need to be implemented in contracts with those organizations to safeguard the security of personal data. In particular, contracts with external organizations must provide that:

13.2.1 the organization may act only on our written instructions;

13.2.2 those processing the data are subject to a duty of confidence;

13.2.3 appropriate measures are taken to ensure the security of processing;

13.2.4 sub-contractors are only engaged with our prior consent and under a written contract;

13.2.5 the organization will assist us in providing subject access and allowing data subjects to exercise their rights in relation to data protection;

13.2.6 the organization will assist us in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;

13.2.7 the organization will delete or return all personal data to us as requested at the end of the contract;

13.2.8 the organization will submit to audits and inspections, provide us with whatever information the Company needs to ensure that both we and the organization are meeting their data protection obligations; and

13.2.9 the organization will notify us immediately if it is asked to do something infringing data protection law.

13.3 Before any new agreement involving the processing of personal data by an external organization is entered into, or an existing agreement is altered, the manager responsible for that must seek approval of its terms by Data Protection Officer and Legal Department.

14 Storage and retention of personal data

14.1 Personal data (and sensitive personal data) will be kept securely in accordance with the Company's Global Information Security Policy.

14.2 Personal data (and sensitive personal data) should not be retained longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal data was obtained. The company ensures that its employees will follow the Company's records retention standards which sets out the relevant retention period, or the criteria that should be used to determine the retention period.

15 Data breaches

15.1 A data breach may take many different forms, for example:

15.1.1 loss or theft of data or equipment on which personal data is stored;

15.1.2 unauthorized access to or use of personal data either by an employee of the Company or third party;

15.1.3 loss of data resulting from an equipment or systems (including hardware and software) failure;

15.1.4 human error, such as accidental deletion or alteration of data;

15.1.5 unforeseen circumstances, such as a fire or flood;

15.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

15.1.7 where information is obtained by deceiving the organization which holds it.

15.2 The Company will:

15.2.1 make the required report of a data breach to the appropriate Supervisory Authority without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of data subjects; and

15.2.2 notify the affected data subjects if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

16 International transfers

16.1 The Company may transfer personal data outside the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein and Norway) to the Company's ultimate parent company on the basis that the Company is designated as having standard data protection clauses**.**

17 Training

The Company will ensure that its employees are adequately trained regarding their data protection responsibilities. Employees whose roles require regular access to personal data, or who are responsible for implementing the Policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

18 Consequences of failing to comply

18.1 The Company takes compliance with the Policy very seriously as failing to comply with it:

18.1.1 puts at risk the data subjects whose personal data is being processed; and

18.1.2 carries the risk of significant civil and criminal sanctions for the individual and the Company; and

18.1.3 may, in some circumstances, amount to a criminal offence by the individual.

18.2 Because of the importance of the Policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures. If a third party breaches the Policy, it may have its contract terminated with immediate effect and potential legal actions may be conducted by the Company.

18.3 If you have any questions or concerns about anything in the Policy, do not hesitate to contact the local Data Protection Offices or Legal Department.