

## Personal data protection policy for external parties (General Data Protection Regulation – GDPR)

### 1. PURPOSE OF THIS POLICY

The European personal data protection regulation (“GDPR” for General Data Protection Regulation) that came into effect on 25 May 2018 provides that natural persons (data subjects) whose data which enables them to be identified (whether directly or indirectly) is processed (whether automatically or otherwise), must be provided with certain information by the data controller responsible for this processing.

The purpose of this policy is to ensure the compliance of MBDA France (hereafter referred to as “**MBDA France**” or the “**Company**”) with this regulation.

This policy describes the nature of the processed data in respect of consultants, temporary staff and other temporary parties not employed by the Company, but pursuing a task within the Company (hereafter referred to as “**External Parties**” or “**you**”), the reasons for processing such data, and the purpose(s) of such processing. In accordance with the GDPR, it also sets out the rights of the data subjects. It is to be noted that neither the data processing carried out nor the information provided regarding these External Parties may imply their integration in the MBDA France employment structure, or the existence of a direct employment contract with MBDA France.

### 2. PRINCIPLES OF PERSONAL DATA PROTECTION

The processing of personal data must comply with certain requirements, particularly those relating to the confidentiality and integrity of the data concerned. These requirements are not new, and pre-existed in previous European and French legislations. As such, MBDA France has always ensured compliance with these regulations (appointment of a Data Protection Correspondent, drafting and implementation of a personal data protection policy, etc.). In this context, MBDA France has carried out appropriate security measures to prevent the personal data of data subjects from being accidentally lost, obtained and/or used in any unauthorised way, or altered or disclosed. The Company also limits data access solely to those employees, agents, subcontractors or other third parties who require such access for clearly defined business reasons. These parties process said personal data only on, and in accordance with, instructions issued by MBDA France, and all are bound by a contractual duty of confidentiality.

In the event of any breach involving your data, you and all relevant regulatory authorities will be informed as required and on every occasion that the Company has a legal obligation to do so.

The GDPR has also confirmed the main principles applying to the processing of personal data. Such data must be:

1. Used lawfully, fairly and transparently
2. Collected solely for specified, precise and legitimate purposes, and not used in any way that is incompatible with these purposes
3. Relevant to the purposes referred to above and limited to the latter
4. Accurate and kept up to date
5. Retained as long as necessary for the achievement of the above mentioned purposes
6. Used in a secure way



The **health and safety**-related activities of the Health, Safety and Environment Department also involve the processing of personal data, particularly in the context of identifying and counting job functions recognised by the relevant regulations as strenuous.

#### 4.2 - Personal data required in the framework of the legal and regulatory defence security requirements and the protection of the nation's scientific and technical assets

The Industrial Security and Defence Department (SID) collects the personal data of External Parties (identification data, access authorisations, access logs) which are related to securing and controlling access to the facilities.

The biometric data (fingerprints) is read for the sole purpose of transfer to the durable medium (badge) where they are stored as a biometric template<sup>2</sup>, that is to say encrypted.

For some External Parties like trainees, where required, SID also collects personal data for the defence clearance requests of the data subject. External Party access permits involve the processing of personal data in preparation for the arrival on Company premises of the concerned External Parties (or in the event of a change in the authorisations granted or the access control methods during their presence within the Company). Clearance requests must be repeated periodically as required, as a consequence so will the collection and the processing of the relevant data be. Such data enables to **ensure the safety of persons and property**. Similarly, SID maintains and monitors the identities of those authorised to access classified documents.

The France Security Directorate also works in conjunction with HR to ensure that those travelling to high-risk countries are fully informed and updated during their stay in such countries. This includes External Parties working on assignment abroad, whose data is collected to ensure the effective **management of the concerned traveling**.

The role of the France Security Directorate through its Information Systems Security department (SSI) is also in conjunction with the IT Directorate to ensure the **security, confidentiality and integrity of telecommunications**. This responsibility requires continuous monitoring of digital data flows within MBDA facilities, as well as inward and outward data flows. These data flows include the identities of both the senders and the recipients. The [MBDA France IT Charter](#) addresses this topic and makes recommendations that must be followed by all users of IT resources.

#### 4.3 – Personal data processed as part of information system development and maintenance

The departments of the IT Directorate monitor data flows to ensure **network and information security**, which includes preventing unauthorised access to our information systems and, more generally, any security failure (data breaches, etc.), as well as the spread of malicious software. Authorised systems and network administrators may intervene to check content or flow volumes identified as suspicious, and are bound by a duty of confidentiality in respect of any data to which they may have had access. These administrators are bound by a duty of confidentiality, and their rights are strictly limited to their intervention perimeter. It is recalled that, in accordance with the Company's [MBDA France IT Charter](#), *“Users must be aware that the majority of their actions in using the information system as well as the data they enter and process within it, including their personal data, are tracked, logged and recorded”*.

---

<sup>2</sup> A biometric "template" refers to the measurements that are stored when registering a person's biometric characteristics (fingerprint). The templates therefore constitute derived biometric data which makes it impossible to reconstitute the original raw biometric characteristic.

#### 4.4 - Cases where you fail to provide us with personal data

External Parties or their employer or the organisation to which they report are required, depending on their status, to provide the relevant departments of MBDA France with the personal data the Company needs to carry out the processing required by law, or that the Company may lawfully require them to provide for the effective management of each contract, or for the proper conduct of their work.

Any failure to provide this data could make it impossible for the Company to properly fulfil its contractual commitments or legal obligations, or to respond to a request submitted by the External Party.

#### 4.5 - Information regarding any change or modification of your data

It is essential that the personal data processed by the Company are accurate and up to date. Depending on his or her status, the External Party must therefore inform the concerned department of any change that might affect their personal data; this requirement applies throughout the period of assignment with the Company.

### 5. THE RIGHTS OF DATA SUBJECTS

The GDPR strengthens the rights of individuals whose personal data is subject to processing (data subjects). It specifies the conditions or procedures for exercising some of these rights.

#### 5.1 - The rights of data subjects

External Parties whose personal data is processed by MBDA France have the following rights:

- **The right of access:** Any External Party has the right to obtain confirmation as to whether or not personal data concerning him or her is being processed and, where that is the case, to obtain access to the said data and obtain a copy of that data.
- **The right to rectification:** Any External Party has the right to obtain the rectification of any personal data concerning him or her that is inaccurate. He or she also has the right to have incomplete personal data completed, including by means of providing a supplementary statement.
- **The right to erasure:** In some cases, any External Party has the right to obtain the erasure of his or her personal data. However, such right is not an absolute right, and MBDA France may have legal or otherwise legitimate reasons to retain such data.
- **The right to restriction of processing:** In certain cases, any External Party has the right to have the processing of his or her personal data limited.
- **The right to data portability:** In certain cases, any External Party has the right to receive his or her personal data provided to MBDA France, in a structured, commonly used and machine-readable format, and to pass such data on to another data controller without hindrance from the Company.
- **The right to object:** Any External Party has the right to object, on grounds relating to his or her particular situation, at any time to the processing of his or her personal data, except where such processing is based on MBDA France's legitimate interests or a legal obligation by which the Company is bound.
- **The right to file a complaint with a supervisory authority:** Any External Party has the right to contact the CNIL to file a complaint against MBDA France's personal data protection practices.
- **The right to issue instructions regarding the use of data after death:** Any External Party has the right to instruct MBDA France regarding the use of his or her personal data after his or her death.

An External Party who, in the circumstances described above, wishes to exercise one of his or her rights, may contact the Data Protection Officer (DPO) by writing to [DPO-fr@mbda-systems.com](mailto:DPO-fr@mbda-systems.com). A data subject access or erasure request form (depending on the nature of the request) will then be proposed to the External Party to help him or her define the request and facilitate the response by MBDA France.

## 5.2 - Free exercise of rights

External Parties are not required to pay a fee when requesting access to their personal data (or exercising any other of their rights). Nevertheless, the Company may charge a reasonable fee where the request is clearly unfounded or excessive. In such circumstances, the Company may alternatively, refuse to process the request.

## 5.3 - Information that the Company may need from External Parties

Where an External Party wishes to exercise one of the above-mentioned rights, the Company may need to request specific information to facilitate the process of his or her identity verification and enable him or her to exercise the right concerned. This request forms part of the security measures put in place to ensure that no personal data is disclosed to a person who isn't authorised to receive it.

## 5.4 - The purposes of the processing

MBDA France uses personal data solely for the purposes for which it was collected and as described in section 4 above. If they were to be used for another purpose that however remains compatible with the original purpose, the data subjects would be informed in advance of this change and of the reasons for it.

## 5.5 - Automated decision-making

Automated decision-making takes place when a computer system uses personal data to make a decision without human intervention. The Company may use such automated decision-making where necessary for business management purposes, subject to appropriate measures having been put in place to safeguard your rights.

## 5.6 - Withdrawal of consent in the specific cases where consent was previously given

Where consent was required for the collection, processing and/or transfer of an External Party's personal data for specific purposes, the latter shall have the right, at any time, to withdraw consent for such processing. He or she may exercise this right of withdrawal by contacting the Data Protection Officer (DPO) by writing to [DPO-fr@mbda-systems.com](mailto:DPO-fr@mbda-systems.com).

On receipt of notification that consent has been withdrawn, the Company will cease to process the data relating to the requesting External Party, unless it has legitimate grounds for continuing to process such data.

## 6. PERSONAL DATA SHARING

MBDA France shares your personal data only with certified and clearly identified recipients, in accordance with the provisions of the applicable data protection legislation.

The Industrial Security and Defence Department (SID) collects and shares with the regulatory authorities the personal data of External Parties related to securing and controlling the access to the facilities (basic controls and Restricted Area controls), and for defence clearance requests. The biometric data and templates of External Responders benefiting from a biometric badge, however, are not stored by MBDA

France and are not transmitted to any third party. Only the service provider in charge of making and delivering badges will have visual access at the time of said making within a framework strictly limited to the latter.

Service providers and subcontractors may also be required to process personal data entrusted to them by MBDA France under the terms of a contract.

Whenever personal data of External Parties is disclosed to third parties, the latter are contractually bound by a duty of confidentiality and storage requirements equivalent to those of MBDA France, mentioned above. In any event, they must return the received data no later than at the end of their service provision. This applies both in France and abroad, including outside the European Economic Area (EEA).

MBDA France calls upon such third parties in areas such as IT systems management and invoicing.

MBDA France is also likely, where appropriate, to share a certain amount of your personal data with the company that employs you or the organisation to which you report (and which must also be considered a data controller).

Furthermore, in certain circumstances, the GDPR requires companies to disclose to third parties the personal data of any person, including External Parties, working on their premises. These circumstances are the following:

- In the event of a merger or acquisition of all or part of the data controller company by a third-party
- In response to judicial or administrative proceedings of any kind, or law enforcement measures instigated by the competent authorities
- To comply with legal obligations, to protect the rights and/or safety of an individual, to protect the rights and the property of MBDA France, including the need to have this policy complied with, and to prevent fraud, security or technical problems.

In the event that it becomes necessary to transfer personal data concerning External Parties to companies located outside the European Economic Area (EEA) that the European Commission does not recognise as providing an adequate level of protection, MBDA France would impose contractual conditions ensuring that these third parties process the data in compliance with EEA legislation and with requirements equivalent to those provided for in French law. You can find copies of such clauses at the following address: <https://www.cnil.fr/fr/les-clauses-contractuelles-types-de-la-commission-europeenne>.

## 7. DATA SECURITY

The Company has put in place measures to preserve the security of the personal data of any person, including External Parties, working on its premises.

Third parties access and process your personal data only on, and in accordance with, instructions issued by the Company, provided that they have committed themselves to maintain the confidentiality of such data and ensure its protection in accordance with all applicable regulations.

Internally, MBDA France has put in place appropriate security measures to prevent the personal data of External Parties from being accidentally lost, used and/or obtained in any unauthorised way, or altered or disclosed. Furthermore, the Company limits the access to such personal data solely to those employees, agents, subcontractors and other third parties who require such access for clearly defined business reasons. These parties process such personal data received from the Company only on, and in accordance with, our instructions, and all are bound by a duty of confidentiality.

Subject to the conditions set out in the applicable legislation, External Parties and any applicable regulator will be informed of any breach pertaining to their personal data.

## 8. DATA RETENTION PERIOD

The Company will retain personal data only for as long as necessary to fulfil the purposes for which it was collected, and will do so in accordance with its contractual, legal and regulatory obligations, internal policies, and accounting as well as financial reporting requirements, in all cases subject to its legitimate interests.

Except in special circumstances which would call for specific clarification, personal data may be stored for the duration of your assignment within the Company and beyond in accordance with the Company's legal obligations and the applicable limitation periods (External Parties' data is therefore generally retained for a period of 5 years following completion of their assignment).

It should be noted that the biometric data necessary for access control are not kept by the Company. The biometric template is stored on the badge held by each External Party (this badge being physically destroyed when the External Party concerned leaves the Company). The identification and logging data, also collected in this context, are kept for a period of six months (i.e. six rolling months for the access logs and six months from the withdrawal of authorisations for the data identification).

## 9. DATA PROTECTION OFFICER (DPO)

A Data Protection Officer (DPO) has been appointed. His role is to ensure that, within MBDA France, all applicable regulations relating to personal data protection are fully complied with. If you have any questions regarding this policy or the way the Company handles your personal data, please contact the DPO at the following address: [DPO-fr@mbda-systems.com](mailto:DPO-fr@mbda-systems.com).

If you have any complaint regarding the protection of your personal data, you may file your complaint with the *Commission Nationale Informatique et Libertés* (CNIL), the French supervisory authority for data protection matters: <https://www.cnil.fr/fr>.

## 10. CHANGES TO THIS POLICY

The Company reserves the right to update this policy where appropriate. Whenever major changes are made to it, a new policy will be issued to you. The Company may also from time to time notify you in other ways about the processing of your personal data.

---