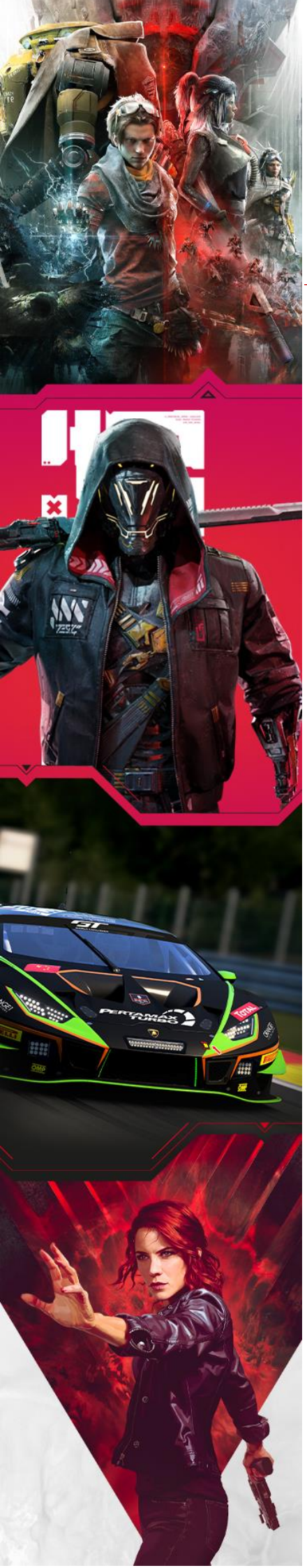

Privacy procedures manual

Digital Bros S.p.A.

Via Tortona, 37 – 20144 Milan, Italy
VAT 09554160151
Share capital: Euro 6.024.334,80 of which Euro 5.706.014,80 subscribed
Milan Companies House no. 290680-Vol. 7394 Chamber of Commerce no.1302132

This manual is available on the Company's website www.digitalbros.com
Privacy & Cookie Policy section

Please consider that this is an Italian to English translation: the Italian version shall always prevail in case of any discrepancy or inconsistency

GLOSSARY

NATURAL PERSON: any single individual;

LEGAL PERSON: companies, associations, bodies or cooperatives with legal personality;

PERSONAL DATA:

- **IDENTIFICATION DATA:** data through which it is possible to obtain the direct identification of the Data Subject (Name, Surname, tax code, Customer Code, etc.)
- **SPECIAL DATA:** data through which is possible to obtain race and ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organizations of a religious, philosophical, political or trade union nature of a person, as well as data pertaining to the health or sexuality of a person;
- **JUDICIAL DATA:** data through which is possible to reveal any judicial measures against the person, in the field of: criminal record, registry of administrative sanctions or the quality of defendant or suspect;

PRIVACY FIGURES:

- **DATA CONTROLLER:** the natural or legal person, public Supervisory Authority, service or other body which, individually or collectively, determines the purposes and means of processing Personal Data.
    - In our case DIGITAL BROS S.P.A..
- **DATA PROCESSOR:** the natural or legal person, public Supervisory Authority, service or other body that processes Personal Data on behalf of the Data Controller.
    - In our case they can be Consultants, Suppliers of goods and services identified in the third party register.
- **DPO:** or Data Protection Officer who assists the Data Controller or manager in monitoring compliance with the applicable legislation on the protection of Personal Data.
    - In our case Veronica Devetag Chalaupka (dpo@digitalbros.com)
- **PRIVACY OWNER:** the person who guarantees the application of security measures and rules for the management and protection of data whose purposes fall under his responsibility.
    - In our case all office managers as well as executives.

- **PRIVACY OFFICER:** the person who defines the corporate processes and procedures to guarantee the correct processing of Personal Data and drafts all the documentation necessary for the fulfillment of privacy matters.
    - In our case the General Counsel Dario Treves.
- **AUTHORIZED:** the individual who, authorized under written appointment, processes the data according to the policies, procedures and rules in force and on indications received from the Data Controller.
    - In our case all Digital Bros S.p.A. employees.
- **DATA SUBJECT:** the natural person who can be, directly or indirectly, identified
    - In our case Employees, customers, suppliers.
- **DPIA/ Data Protection Impact Assessment:** a more in-depth impact analysis finalized to identify the measures to contain and protect the data of the interested parties.

*****

DATA BREACH MANAGEMENT

GENERAL PRINCIPALS

A data breach is a particular type of security incident, as a result of which, the Data Controller is unable to guarantee compliance with the GDPR "Principles applicable to the processing of Personal Data".

A Personal Data breach arises from situations in which Personal Data, whether in electronic or physical form, is subject to:

- breach of Confidentiality: when unauthorized or accidental disclosure or access to Personal Data occurs;
- breach of Integrity: when unauthorized or accidental alteration (modification) of Personal Data occurs;
- breach of Availability: when accidental or unauthorized loss, inaccessibility, or destruction of Personal Data occurs;

Art. 33 of the GDPR establishes that, in the event of a Personal Data breach, the Data Controller must notify the competent Supervisory Authority of the breach without unjustified delay and, where possible, within 72 hours from the moment in which he became aware of it, unless the Personal Data breach is unlikely to present a risk to the rights and freedoms of Data Subjects (Natural Persons). The Data Controller must document any event that could potentially be configured as a Data Breach, also keeping

as reference the indications contained in the Guidelines issued by the "Article 29 Data Protection Working Party" - WP29 group[1] (paragraph II, clause 2[2]), which provide for exceptions from the notification obligation to allow the Supervisory Authority itself to verify overall compliance with the legislation.

In the event of a high risk for the rights and freedoms of individuals, the Data Controller must also notify the interested parties (Art. 34).

Digital Bros S.p.A. must therefore notify the Supervisory Authority of any violations of Personal Data (following computer attacks, abusive accesses, accidents or natural disasters, such as fires or floods) that may "jeopardize" the freedoms and rights of the subjects concerned. Therefore, the general activities of Detection, Evaluation, Notification and Monitoring of the breach must be documented, detailed, traceable, replicable and cannot be modified in the event of verification by the Supervisory Authority.

It is important that the moment of discovery of the data breach (moment in which the Data Controller becomes aware and has had a reasonable degree of certainty that the violation has occurred) can be demonstrated, as the 72 hours for notification start from that moment.

The WP29 Guidelines clarify that the identification of the moment from which, a Data Controller can be considered "aware" of a particular violation will depend on the circumstances of the specific violation. In the event of Personal Data breaches which could pose a risk to the rights and freedoms of Data Subjects, then Digital Bros shall:

- notify the Supervisory Authority of the Personal Data breach within 72 hours; and
- communicate, where applicable and without undue delay, to all interested parties involved, the violation (said condition applies only in the event that the data breach could involve a high risk for the rights and freedoms of the subjects involved).

Should the notification to the Supervisory Authority not be made within 72 hours, the Data Controller will have to provide the reasons for the delay (e.g. problems in collecting all the information necessary for the notification).

Where it is not possible to provide all the information requested at the time of notification, it will need to be supplemented as soon as it is available.

[1] Consultative and independent body, composed of a representative for each of the personal data protection authorities designated by each Member State, by the EDPS (European Data Protection Supervisor), as well as by a representative of the European Commission. Among the most relevant tasks among those regulated, it appears to formulate recommendations on one's own initiative on any matter concerning the protection of personal data in the European Community.

[2] Guidelines on Personal data breach notification under Regulation 2016/679 – adopted on February 6th, 2018

DATA BREACH MANAGEMENT

The Data Breach management process planned by Digital Bros consists of four main phases, illustrated in the following paragraphs:

a. **Detection**

b. **Evaluation**

c. **Notification**

d. **Monitoring**

DETECTION

The main detection methods that can lead to the identification of a violation can consist of:

- Reports to the IT Systems Manager, for issues relating to logical security (such as, for example, the identification of a violation through analysis tools and/or verification, control and monitoring activities of the IT infrastructure);
- Reports to the Physical Systems Manager for issues relating to physical security of physical archives (such as, for example, the identification of a physical incident through verification and control activities).

Reports can be submitted by several different sources:

- reports from employees or other personnel (for example consultants or independent subjects) who work for Digital Bros S.p.A.;
- reports from third parties such as customers, suppliers and other parties that do not have direct relationships with Digital Bros S.p.A., including reports received directly from the Supervisory Authority or from other public bodies (Postal Police, etc.,);
- reports received from persons appointed as External Data Processors.

All Digital Bros employees must be aware of the importance of paying attention to what could constitute a Data Breach, its potential threats and how to promptly report the event to the indicated subjects, who will immediately notify the Privacy Officer and the DPO.

REPORTING TO COMPETENT FIGURES

i. Reporting by an employee

If an employee detects an incident / breach of logical (e.g. cyber-attack, theft of a laptop, etc.) or physical (e.g. fire or flooding of a building containing documentation) security which also leads to accidental destruction, loss, unauthorized modification, disclosure and access to Personal Data transmitted, stored or otherwise processed, it is necessary that the findings be promptly reported to the IT Systems Manager (for issues relating to logical security) or the Physical Systems Manager (for topics related to physical security / of physical archives).

However, if an autonomous subject, such as a consultant working for Digital Bros S.p.A., detects a breach of Personal Data security, he must promptly notify his internal representative, who will forward the relative report following the procedure described above.

ii. Reporting by a third party

If the Data Breach detected by a third party, such as a customer, is reported via any Digital Bros S.p.A. contact channels (e.g. telephone, email, etc.), the employee who receives the communication must promptly notify and report it following the procedure described above (paragraph i. Reporting by an employee).

iii. Notification by an External Data Processor

The External Data Processor must notify his contractual representative (a figure who maintains relations with the External Data Processor himself) of any breach of security which also involves the accidental destruction, loss, unauthorized modification, disclosure or access to the Personal Data transmitted, stored or otherwise processed in the context of the supply, within a maximum of 24 hours from the detection of the event. Digital bros S.p.A. employee, who receive the communication as the contractual representative of the External Data Processor, must promptly communicate and report the data breach following the procedure described above (paragraph .i. Reporting by an employee).

The External Data Processor, following the report, supports the Privacy Officer in the assessment process by collecting all the information necessary to allow, in a complete and timely manner, any notification of the violation to the Supervisory Authority and, where necessary, the communication to the subject involved.

The External Data Processor is required to respond promptly to every request for information received from the Data Controller.

INCIDENT DETECTION IN THE CONTEXT OF MONITORING ACTIVITIES

In order to be able to detect a violation of Personal Data in a timely manner in compliance with the applicable regulatory requirements, Digital Bros S.p.A. has provided for the implementation of organizational and technical measures to identify and prevent any incidents, in compliance with the principle of proportionality.

The IT Systems Manager provides organizational and technical measures (for example procedures, intrusion prevention and detection tools, etc.) to prevent, detect and report any incidents falling within the IT sphere.

The Physical Systems Manager, using the tools used to protect the physical archives managed and within the perimeter of the physical security of his competence, could detect the occurrence of an incident, with a potential impact on Personal Data. In this case he will report the potential Data Breach to the Privacy Officer who, after appropriate evaluation, will start the Data Breach process, involving the competent figures.

STARTING THE DATA BREACH MANAGEMENT PROCESS

Based on the reports received and/or those detected by the IT Systems Manager and the Physical Systems Manager according to the methods referred to in paragraph i, the Privacy Officer will carry out an initial rough evaluation, with the support of the DPO, to determine whether the event in question can be assessed as a potential Data Breach.

To this end, the Privacy Officer may send any requests for further information to the various Privacy Owners of the areas involved and, if necessary, to the IT Systems Manager and to the Physical Systems Manager.

The Privacy Owners of the areas involved collect the information necessary for the evaluation of the event requested by the Privacy Officer, supported, where necessary, by the IT Systems Manager and the Physical Systems Manager.

In order to analyze the possible Data Breach event, the following minimum information should be acquired in the Information Collection Form:

- *Date and time it occurred*
- *Date and time it was detected*
- *Who / what reported it*
- *Description of the nature of the violation*
- *Approximate number and category of Data Subjects involved*
- *Approximate number and category of Personal Data breached*

- *Details of the affected IT system(s)*
- *Physical storage or removable devices involved*
- *Security measures in place*
- *Material to support the detection, such as error messages, LOGs, etc.*
- *Measures taken or proposed to be taken to reduce the impact or remedy the Data Breach.*

In order to allow a complete analysis of the Data Breach, the utmost attention must be paid to ensuring that the information is always updated, meticulously collected and promptly shared with all the parties involved in the management of the event, making sure that the most complete and up-to-date overview is always available.

In the event that, following the general evaluation, the event is assessed as a potential Data Breach, the Privacy Officer convenes the Data Breach Management Committee (as described in the following paragraph). The Data Breach Management Committee shall then analyze the information collected and evaluate whether or not to proceed with the notification to the Supervisory Authority and/or the Data Subject.

THE DATA BREACH MANAGEMENT COMMITTEE

The purpose of the Data Breach Management Committee is to evaluate the event detected and identify the actions to be taken shall the event be classified as a Data Breach.

The Data Breach Management Committee:

- Analyzes the event;
- Evaluates whether it should be classified as a Personal Data breach;
- Evaluates whether it is necessary to notify the Supervisory Authority;
- Evaluates whether it is necessary to notify the interested parties;
- Identifies the mitigation measures to implement.

The Data Breach Management Committee comprises the following functions:

- DPO
- Privacy Officer
- IT Systems Manager
- Physical Systems Manager
- System Administrator
- Any other individual whose participation shall be considered based on each circumstance, such as:
    - Privacy Owner involved in the event.

EVALUATION

The Data Breach Management Committee carries out an evaluation assessment of the event, in order to identify the presence and level of risk for the rights and freedoms of the interested parties.

To assess the level of risk it is necessary to consider the following:

- Type of information / data involved (e.g. name and surname, domicile or other residential addresses, information on age, gender, email addresses, telephone numbers, passport number, driving license, sensitive personal information, etc.)
- Security mechanisms in place (e.g. access control, encryption, etc.)
- Data subjects affected by the breach (e.g. number of Data Subjects, name, contacts, etc.)
- Actions to be taken or already in progress to mitigate losses and limit the impact of the Personal Data breach (e.g. blocking access to specific systems, system updates, etc.)
- Potential negative consequences, associated with the actual compromise, for the subjects involved.

Recital 88 of the GDPR specifies that due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse.

FACTORS TO CONSIDER WHEN EVALUATING A DATA BREACH RISK

Recitals 75 and 76 of the GDPR suggest that, in assessing the risk, both the severity/impact that the same would entail for the rights and freedoms of the Data Subjects, and the likelihood of the same happening should be taken into consideration.

Risk should also be evaluated on the basis of an objective assessment.

When assessing the risk that could arise from an infringement, the Data Controller should consider a combination of the severity of the potential impact on the rights and freedoms of natural persons and the likelihood that they will occur. Where the consequences of a breach are more severe, the risk is higher, and similarly, where the likelihood of this happening is higher, the risk also increases.

In order to adequately assess the risk associated with the “data breach” under analysis, specific factors must be analyzed, namely:

Factor to consider	Evaluation scope
Type of violation	Define the type of violation in terms of Confidentiality, Integrity and Availability.

	For example, a breach of confidentiality, whereby information has been disclosed to unauthorized parties, may have different consequences for an individual than a breach in which an individual's information has been lost and is no longer available.
Nature, type and volume of Personal Data	Identify the nature (e.g. type of Personal Data), the type (e.g. data that can detect an individual's racial origins) and volume (in terms of quantity) of Personal Data breached. The more types of data involved, the greater the potential risk for Data Subjects. In addition, other aspects relating to the data processed must also be taken into consideration, such as: • The disclosure of an individual's name and address is unlikely in ordinary circumstances to cause substantial harm, however, if an adoptive parent's name and address were disclosed to a natural parent, the consequences could be profoundly serious both for the adoptive parent for the child; • A list of customers requesting regular deliveries might not be particularly sensitive, but the same data about customers who have requested their deliveries to be stopped during the holidays would be useful information for criminals.
Ease of identification of people	Detect the ease with which it is possible to identify a subject or if the information in question can allow the identification of a specific individual and with how much precision it is possible to do so. For example, the ease with which an attacker can access Personal Data to identify specific individuals or match the data with other information to identify individuals. Depending on the circumstances, identification could be possible directly from the Personal Data being breached without any specific research needed to discover the identity of the individual, or it could be extremely difficult to match the Personal Data to a particular individual, but it could still be possible to certain conditions (e.g. knowledge of the decryption key).
Severity of the consequences for individuals	Identify the consequences for individuals deriving from the violation and the relative severity. Depending on the nature of the Personal Data involved in a breach, for example, special categories of data, the potential harm that could result to individuals could be particularly severe, particularly where the breach could involve identity theft or fraud, physical harm, psychological distress,

	humiliation or damage to reputation. If the violation concerns Personal Data of vulnerable individuals (e.g. minors), they could be exposed to a greater risk of damage.
Special characteristics of the individual	Detect the presence of individuals with special characteristics, such as minors or disabled persons. A breach may affect Personal Data relating to children or other vulnerable people (e.g. disabled people), as a result these subjects could be exposed to greater dangers.
Particular characteristics of the Data Controller	Define the characteristics of the Data Controller (e.g. hospital clinic). Following a breach, the nature and role of the Data Controller and its activities can affect the level of risk to individuals. For example, a medical organization processes special categories of Personal Data, which means that there is a greater threat if people's Personal Data is breached than if a newspaper mailing list is breached.
Number of individuals involved	Define the number of individuals involved. A breach may affect only one or a few individuals or several thousand, if not more. Generally, the more individuals affected, the greater the impact of a breach. However, a breach can have a serious impact even on one individual, depending on the nature of the Personal Data and the context in which the data was breached.
Security measures in place to protect data	Identify the security measures in place to protect the Personal Data. For example, Personal Data protected by an appropriate level of encryption, without the decryption key, will be incomprehensible to malicious parties and/or parties without authorization to access such data. Likewise, Personal Data protected by pseudonymization, implemented in a way that prevents Personal Data from being attributed to a specific Data Subject without the use of additional information (which is kept separately), can also reduce the likelihood that individuals will be identified in case of violation. However, pseudonymization techniques alone cannot be considered as intelligible.
Security measures to be implemented for data protection	Identify the security measures that must be implemented and adopted to protect the data.

	For example, if a system vulnerability is discovered, it will be necessary to promptly update it (patch management).

Based on the analysis of the factors listed above, for each violation it is necessary to evaluate the Impact and Probability relating to the risks for the interested parties. The possible evaluation levels associated with the impact itself are shown below.

Impact	Description of the impact	Value
Low	Individuals will not be impacted by the breach or may be impacted by some unnecessary inconvenience, which they will be able to easily overcome (e.g. time spent re-entering information, annoyances, irritations, etc.)	1
Medium	Individuals may experience significant hardships, which they will be able to overcome despite some difficulties (e.g. fear, lack of understanding, stress, minor physical ailments, etc.)	2
High	Individuals may face significant consequences, which they should be able to overcome albeit with great difficulty (e.g. misappropriation of funds, bank blacklisting, property damage, job loss, lawsuit, illness, etc.)	3
Very high	Individuals may encounter significant, or even irreversible, consequences that are impossible to overcome (financial hardship such as substantial debt or incapacity to work, long-term psychological or physical ailments, death, etc.)	4

Following the assessment of the impact of the data breach, the probability that the identified impact will occur must be assessed, i.e. whether the threat can occur or not.

Probability	Description of the probability	Value
Low	The threat/risk cannot occur Threat/risk may not occur or is remotely likely to occur	1
Medium	The threat/risk is likely to materialize	2
High	Threat/risk will surely occur eventually	3
Very high	The threat will certainly materialize in the near future	4

The classification level of the violation is obtained multiplying the value assigned after the impact and probability assessment, using the formula "IxP" (impact * probability). Below is the range through which it is possible to assign a classification to the data breach.

Classification	Risk range	Notes for classification
Negligible risk	Final value between 1 and 3 included	No form of risk for data security, which involves the accidental or unlawful destruction, loss, modification, unauthorized disclosure or access to Personal Data transmitted, stored or otherwise processed, is detected.
Presence of risk	Final value between 4 and 11 included	Violation of common personal information (e.g. identification data) There will be a potential impact on the privacy of the people involved (e.g. spam activity)
Presence of high risk	Final value between 12 and 16 included	Violation of sensitive personal information (e.g. health, financial, judicial data) There is potential for identity theft There will be a high impact on the privacy of the people involved due to the impairment of sensitive Personal Data (e.g. Spearphising activity)

The data breach must be notified to the Supervisory Authority and, if necessary, to the Data Subjects, following the general classification of the risk previously conducted. Below the actions to be taken based on the result of the classification.

Classification	Action to be taken
Negligible risk	There is no obligation to notify the Supervisory Authority The violation is logged and documented
Presence of risk	There is an obligation to notify the Supervisory Authority The violation is logged and documented
Presence of high risk	There is an obligation to Notify the Supervisory Authority After having notified and consulted the Supervisory Authority, the violation must be communicated to the interested parties

	The violation is logged and documented

The Data Controller, with the support of the Committee, shall then decide if a notification to the Supervisory Authority is needed and, if the conditions are met, also to the Data Subject. For example, in the event of a "high risk for the rights and freedoms" of the Data Subject, the Committee shall also take into consideration the following when assessing the need to proceed with the notification:

- communication to the Data Subject is not required if one of the following conditions is met:
    - adequate technical and organizational measures for the protection of Personal Data have been put in place and these measures have been applied to the Personal Data subject to the breach, in particular those intended to make the Personal Data incomprehensible to anyone who is not authorized to access it, such as the encryption;
    - measures have been taken to prevent the occurrence of a high risk for the rights and freedoms of the Data Subjects;
    - the communication would require disproportionate efforts; in this case, instead, a public communication or a similar measure is carried out, through which the Data Subjects are informed with similar effectiveness. Possible factors to be taken into consideration in evaluating this case could be, among others, costs, time, difficulty in providing information, etc.

The need to mitigate an immediate risk would require timely communication to the Data Subjects, while the need to implement appropriate measures to counter repeated or similar Personal Data breaches may justify a delay in communication also in order not to hinder the investigation activities.

NOTIFICATION

As described below, the Data Breach Management Committee, based on the result of the risk assessment of the Personal Data breach, will initiate the Internal Approval process and the External Notification and Communication process, if necessary.

A. INTERNAL APPROVAL

The internal reporting activities to be performed by the Committee are set out below.

The Data Breach Management Committee shares with the Data Controller the status of any data breaches classified as:

- violation with Presence of Risk;

- violation with High Risk Presence.

In such context, the Data Breach Management Committee also presents to the Data Controller the mitigation measures already in place and those envisaged to mitigate the risk.

Based on the Risk Classification, a report of the determinations is drawn up and the decision of the Data Controller is noted; copy of the report is kept by the DPO.

B. NOTICE AND EXTERNAL COMMUNICATION

In case of approval, the DPO, with the support of the Privacy Coordinator, manages both the Notification to the Supervisory Authority and the communication to the Data Subject.

The types of communication flows towards the outside are shown below:

- notification to the Supervisory Authority;
- communication to Data Subjects, where applicable.

Notification process to the Supervisory Authority

The DPO, on the basis of what has been decided, notifies the Supervisory Authority of what happened, using the channels and/or forms provided, possibly defined by the Supervisory Authority. The Data Breach Management Committee supports the DPO in the notification process.

The notification must:

- describe the nature of the Personal Data breach including, where possible, the categories and approximate number of Data Subjects concerned as well as the categories and approximate number of records of the Personal Data concerned;
- communicate the name and contact details of the DPO or other contact point where more information can be obtained;
- describe the likely consequences of the Personal Data breach;
- describe the measures taken or proposed to be taken to deal with the Personal Data breach, including, where appropriate, measures to mitigate its possible negative effects.

Given the importance of timely communication to the Supervisory Authority if, and to the extent that, it is not possible to provide all the information at the same time as the first notification, further information will be forwarded as soon as it is available. Delay in the notification by the Data Processor to the Supervisory Authority may be delayed due to the:

- complexity and number of systems (also considering those used by third parties), as well as the data they process;

- discovery of multiple violations, thus allowing an "aggregate" notification instead of an individual one;
- discovery of multiple breaches involving the same types of data that occurred within close proximity of each other.

The need to aggregate multiple notifications does not necessarily lead to a delay in notification to the Supervisory Authority.

Communication process to Data Subjects

When the Personal Data Breach (assessed through the procedure described above) could lead to a high risk for the rights and freedoms of the Data Subjects or at the request of the Supervisory Authority, Digital Bros S.p.A., after promptly notifying the Supervisory Authority of the event, communicates the violation of Personal Data to the Data Subjects without undue delay. The Data Breach Management Committee establishes the most appropriate channel for sending this communication (e.g. e-mail, SMS, telephone, etc.). When several Data Subjects are involved, Digital Bros S.p.A. will inform, the subjects whose data are affected by the violation through forms of communication of a public nature, such as the dissemination of notices in newspapers, including online, or through other available tools, as soon as reasonably feasible and in close collaboration with the Supervisory Authority (Recital 86 of the GDPR).

The communication to the Data Subject must at least:

- describe, in simple and clear language, the nature of the Personal Data breach including, where possible, the categories and approximate number of individuals affected, as well as the categories and approximate number of Personal Data records affected;
- communicate the name and contact details of the DPO or other contact point where further information can be obtained;
- describe the likely consequences of the Personal Data breach;
- describe the measures adopted or proposed to be adopted to deal with the Personal Data breach, including, where appropriate, suggesting measures to mitigate the possible negative effects.

VIOLATION MONITORING

The violation monitoring phase comprises the following activities:

- The IT Systems Manager or the Physical Systems Manager who reported the incident relating to the management of their archives / physical and / or logical security to the Privacy Officer (with the support of any relevant functions) constantly analyzes the event and provides

additional and updated information, taking action to resolve the violation while updating the Committee on the progress of the management and resolution of the Data Breach;

- The Data Breach Management Committee monitors the progress and evolution of the violation by requesting and receiving additional and necessary information from time to time. In addition, the Committee evaluates the mitigation measures necessary for the protection of the Personal Data of the Data Subjects;
- The IT Systems Manager or the Physical Systems Manager to whom the incident relating to the management of physical archives/physical security refers, after having identified and remedied the vulnerability(s) evolved in Data Breach, supports the DPO in the filing and constant updating of the Data Breach Register, regarding:
    - description of the Data Breach;
    - nature of the violation;
    - root cause analysis;
    - action plan aimed at securing Personal Data;
    - corrective actions implemented or in the process of being implemented.
- The Data Breach Management Committee informs the Data Controller of the closure and resolution of the violation;
- Once the evaluation process is concluded and all the information has been collected, the DPO prepares a Data Breach closure report which must contain at least:
    - Description of the nature of the Data Breach;
    - Date and time the Data Breach was detected;
    - Who / what reported the Data Breach;
    - Approximate number and category of Data Subjects involved;
    - Approximate number and category of Personal Data breached;
    - Details of any IT system involved;
    - Physical storage or removable devices involved;
    - Security mechanisms in place at the time of the Data Breach;
    - Possible consequences of the Data Breach;
    - Measures taken or likely to be taken.
- The IT Systems Manager or the Physical Systems Manager also implements the identified security measures.
- The DPO, together with the members of the Data Breach Management Committee, evaluates the training needs of the employees, in particular with reference to what emerged from the analysis of the violation.

- The DPO manages the correspondence and feedback received from the Supervisory Authority such as methods and times for communication to the interested parties, security measures to be implemented, etc.

As part of the Data Breach monitoring activities, a register containing all the information relating to the violations ("Data Breach Register") is filed. The Data Breach Register shall at least contain:

- the documentation relating to the Data Breach (information collected, evaluations carried out and any other material to support the evaluation, such as for example error messages, LOGs, etc.);
- notification of the violations filed with the Supervisory Authority;
- the communication of the violations to the Data Subjects, where applicable;
- feedback received from the Supervisory Authority.

DATA BREACH REGISTER MANAGEMENT

In order to allow the Supervisory Authority to verify compliance with the law, the DPO records and archives any violation of Personal Data in the Data Breach Register, also entering the events for which it was decided not to proceed with the notification and the reasons for this choice.

The Data Breach Register must be continuously updated and made available to the Supervisory Authority, should the latter request it.

Suitable measures must be taken to guarantee the integrity and non-modifiability of the records contained therein.

DATA RETENTION

GENERAL PRINCIPLES

This paragraph describes the retention times of the various types of Personal Data for which Digital Bros S.p.A. classifies as Data Controller and which are processed by various Digital Bros S.p.a. functions in charge of Personal Data management, in accordance with the provisions of current legislation on Personal Data protection (EU Regulation 2016/679).

The provisions therein apply to the data of:

- Candidates;
- Employees;
- B2C & B2B customers;
- Suppliers;
- Visitors.

The document provides the necessary indications for the deletion of data, according to the retention period indicated. The provisions also apply to all third parties (customers, suppliers, consultants, agents, etc.) who participate in the conservation and cancellation of Personal Data owned by Digital Bros.

STORAGE OF PERSONAL DATA

Digital Bros must define the retention period of Personal Data, after which the cancellation or anonymization must be carried out according to the applicable legislative and regulatory provisions. These laws and regulations may have specific requirements relating to the processing of Personal Data (e.g. marketing or profiling activities).

Digital Bros must at least:

- keep Personal Data only for the time necessary to complete the activities for which the data were collected, and which were declared in the privacy policy delivered to the interested parties;
- keep Personal Data ensuring compliance with the consent obtained from the individual and with contractual and legislative requirements;
- delete Personal Data if required by local regulatory requirements;
- delete Personal Data if the Data Subject wishes to exercise the right to cancel all Personal Data concerning him without unjustified delay ("right to cancellation") and communicate the request of the Data Subject and to any third party to whom the Personal Data are been communicated, if applicable.

Furthermore, following a request for cancellation by the Data Subject, Digital Bros must guarantee this right when at least one of the following points applies:

- Personal Data are no longer necessary with respect to the purposes for which they were collected or otherwise processed;
- the Data Subject revokes the consent on which the treatment is based and if there is no other legal basis for the treatment;
- the Data Subject opposes the processing and there is no overriding legitimate reason to proceed with the processing;
- the Personal Data have been processed unlawfully;
- Personal Data must be erased to fulfill a legal obligation under national laws and regulations to which Digital Bros is subject;
- the retention of Personal Data violates national laws and regulations to which Digital Bros is subject.

The Data Subject could also exercise his right to portability. In this case, it does not automatically change the defined retention period and does not automatically cause the deletion of Personal Data from Digital

Bros systems, until the Data Subject present a specific request. In the event that the Data Subject, on the other hand, exercises the right to limitation, the possible expiry of the term or other conditions that could require the cancellation of the data would remain suspended until the termination of the constraint itself.

CANCELLATION OF PERSONAL DATA

At the end of the retention period, Digital Bros must delete the Personal Data collected in accordance with the applicable laws and regulations.

Digital Bros must also communicate, without unjustified delay, to any third party involved in the processing of Personal Data to proceed with the cancellation of the same.

If the deletion of the data is effected, Digital Bros shall not further process such Personal Data. For this reason, Digital Bros must implement processes and mechanisms to ensure that deletion periods are periodically reviewed and the final time limits for deletion of Personal Data are respected, internally and externally (e.g. by third parties who process Personal Data), including specific contractual clauses that allow Digital Bros to conduct audit activities.

Digital Bros must also ensure that all electronic devices where Personal Data has been stored are, at the end of their life cycle, carefully disposed of, in order to prevent any unauthorized access to the information stored within them.

DATA RETENTION

The tables shown below in the document contain an indication of the retention period of the data processed with reference to the various categories of Data Subjects:

- Applicants
- Employees
- B2C & B2B customers
- Suppliers
- Visitors
- Other

The retention period indicated therein takes into account any regulatory provisions or specific indications provided by the Supervisory Authority in the provisions issued over the years.

In the absence of indications provided by the applicable legislation or by the Supervisory Authority regarding the retention period of the Personal Data processed, the same was identified by evaluating what could be a suitable period, in compliance with the principle according to which Personal Data

should be kept for the period of time strictly necessary to complete the activities for which they originally were collected.

Finally, it should be noted that all data that does not fall within the categories listed below must be assessed by the DPO and the Privacy Officer, in order to identify the correct retention period.

A. APPLICANTS' DATA

APPLICANTS			
Description and purpose	**Type of data**	**Retention period**	**Regulatory references**
Ordinary and / or "special" Personal Data contained in the curricula, processed for personnel selection purposes	Personal data, contact details, legally protective status, professional experience, education	6 months from the last CV upload	-
Ordinary Personal Data processed for the management and reception of subjects who access the company headquarters	Registry	3 months	-

B. EMPLOYEES' DATA

EMPLOYEES			
Description and purpose	**Type of data**	**Retention period**	**Regulatory references**
Ordinary and/or Special Personal Data relating to the employees processed for the purpose of managing the contractual relationship (for example, the management of payroll, etc.)	Personal data, contact details, employment contract, employee personal file, disciplinary documentation, copy of identity document and educational qualification, membership of trade unions, certificates of participation in training courses, pay slips, remuneration, benefits, pension, salary data	At least 10 years after the end of the contractual relationship, subject to retention for tax purposes	*This period is determined pursuant to art. 43 of Presidential Decree 600/73 and art. 2946 of the Italian Civil Code on ordinary prescription**

EMPLOYEES			
Description and purpose	**Type of data**	**Retention period**	**Regulatory references**
Ordinary Personal Data processed for the management of complaints and disputes	Personal data, contact details, employment contract, employee personal file, disciplinary documentation, copy of identity document and educational qualification, membership of trade unions, certificates of participation in training courses, pay slips, fees, benefits, regime pension, salary data	At least 10 years after the end of the contractual relationship (to keep the data necessary for the establishment, exercise or defense of a right in court)	*This period is determined pursuant to art. 2946 of the Italian Civil Code on ordinary prescription.* *
Ordinary and/or Special Personal Data relating to health/sanitary aspects processed for the purpose of managing the contractual relationship	Personal data, contact details, presence/absence data, certificates of illness, fitness, disability, paternity/maternity leave, declarations of accidents at work	At least 10 years after the end of the contractual relationship	*This period is determined pursuant to art. 2946 of the Italian Civil Code on ordinary prescription and articles 25 "Competent doctor", 41 "Health surveillance" and 53 "Document keeping" of Legislative Decree 81/08 and subsequent amendments**
Ordinary Personal Data, for the management of tracking of AdS activities, processed for the purpose of managing the contractual relationship	Access log at system and application level for monitoring AdS activities	Minimum 6 months up to a maximum of 24 months from the generation of the log itself	*Supervisory Authority "System administrators" provision of November 28th, 2008 and subsequent amendments**
Ordinary Personal Data processed for the management of the employee's e-mail account	Name, surname, contact details, job title, e-mail address	For the entire duration of the employment relationship and deactivation of the e-mail account upon termination of	-

EMPLOYEES			
Description and purpose	**Type of data**	**Retention period**	**Regulatory references**
		employment within 30 days, in such a way as to definitively inhibit the receipt of incoming messages addressed to the former employee's account, as well as the storage of the same on company servers	
Personal Data processed through video surveillance systems for security purposes and protection of company assets	Images	Maximum 48 hours	*General provision issued by the Supervisory Authority on April 8th, 2010*
Personal Data of Digital Bros S.p.A. Directors and their family unit (except for underage children) for the purpose of issuing the declarations necessary for participation in public tenders (e.g. anti-mafia declaration)	Personal data, contact data, judicial data, tax data	At least 10 years after the end of the contractual relationship	-

C. B2C CUSTOMERS' DATA

B2C CUSTOMERS			
Description and purpose	**Type of data**	**Retention period**	**Regulatory references**
Ordinary Personal Data processed for direct marketing purposes	Personal data, contact details	2 years from the withdrawal of consent	-
Ordinary and particular Personal Data processed for	Personal data, contact details	2 years from the fulfillment of the customer's request	-

B2C CUSTOMERS			
Description and purpose	**Type of data**	**Retention period**	**Regulatory references**
customer care purposes (Facebook)			
Ordinary Personal Data processed for the management of complaints and disputes	Personal details, contact details, billing details	At least 10 years after the end of the contractual relationship (to store the data necessary for the establishment, exercise or defense of a right in court)	*This period is determined pursuant to art. 2946 of the Italian Civil Code on ordinary prescription.* *

D. B2B CUSTOMERS' DATA

B2B CUSTOMERS			
Description and purpose	**Type of data**	**Retention period**	**Regulatory references**
Ordinary Personal Data of B2B customers	Personal details, contact details, billing details	3 years from the end of the commercial relationship	-
Ordinary Personal Data processed for the purposes of sales accounting and fraud prevention	Personal details, contact details, billing details	At least 5 years after the end of the contractual relationship	*This period is determined pursuant to art. 2948 of the Italian Civil Code which provides for a 5-year limitation period for periodic payments.**
Ordinary Personal Data processed for administrative and tax management purposes and for the management of complaints and disputes	Personal data, contact data, billing data, contracts for goods and services, invoices for goods and services, insurance/guarantee policies, Customer list, permits, licenses, certifications,	At least 10 years after the end of the contractual relationship	*This period is determined pursuant to art. 2946 and art. 2220 of the Italian Civil Code and art. 22 of Presidential Decree 600/1973 (civil obligations of the entrepreneur to preserve accounting records and commercial*

B2B CUSTOMERS			
Description and purpose	**Type of data**	**Retention period**	**Regulatory references**
	confidentiality agreements/MOUs.		*correspondence; conservation obligations for tax purposes).* *
Ordinary Personal Data processed for the management and reception of subjects who access the company headquarters	Registry	3 months	-

E. SUPPLIERS'/EXTERNAL CONSULTANTS' DATA

SUPPLIERS/EXTERNAL CONSULTANTS			
Description and purpose	**Type of data**	**Retention period**	**Regulatory references**
Ordinary Personal Data processed for the management of complaints and disputes	Personal details, contact details, billing details	At least 10 years after the end of the contractual relationship	*This period is determined pursuant to art. 2946 of the Italian Civil Code on ordinary prescription.* *
Ordinary Personal Data processed for administrative and fiscal management	Personal data, contact details, contracts for goods and services, invoices for goods and services, insurance and surety policies, list of customers and suppliers, permits, licenses, certifications, confidentiality agreements/MOUs.	At least 10 years after the end of the contractual relationship	*This period is determined pursuant to art. 2220 of the Italian Civil Code and art. 22 of Presidential Decree 600/1973 (civil obligations of the entrepreneur to preserve accounting records and commercial correspondence; conservation obligations for tax purposes).* *
Ordinary Personal Data, for the management of tracking of AdS activities,	Access log at system and application level for monitoring AdS activities	Minimum 6 months up to a maximum of 24 months	*Supervisory Authority "System administrators" provision of November*

SUPPLIERS/EXTERNAL CONSULTANTS			
Description and purpose	**Type of data**	**Retention period**	**Regulatory references**
processed for the purpose of managing the contractual relationship		from the generation of the log itself	*28th, 2008 and subsequent amendments**
Ordinary Personal Data processed for the management and reception of subjects who access the company headquarters	Registry	3 months	-
Ordinary Personal Data relating to the management of external consultants processed for the purpose of managing the contractual relationship, complaints and disputes and for administrative/tax purposes	Personal data, contact data, billing data, contracts for goods and services, invoices for goods and services, insurance and surety policies, list of customers and suppliers, permits, licenses, certifications	At least 10 years after the end of the contractual relationship	*This period is determined pursuant to art. 2946 of the Italian Civil Code on ordinary prescription and art. 2220 of the Italian Civil Code and art. 22 of Presidential Decree 600/r 1973 (civil obligations of the entrepreneur to preserve accounting records and commercial correspondence; conservation obligations for tax purposes). *

F. VISITORS' DATA

VISITORS			
Description and purpose	**Type of data**	**Retention period**	**Regulatory references**
Ordinary Personal Data processed for the management and reception of subjects who	Personal data, any company you belong to	3 months	-

access the company headquarters			
Personal data processed through video surveillance systems for security purposes and protection of company assets	Images	48 hours	*General provision issued by the Supervisory Authority on April 8th, 2010*

EXAMPLES OF DATA DELETION TECHNIQUES AND DEVICE DISPOSAL

Specific data deletion and device disposal activities must be conducted in order to ensure that Personal Data is no longer accessible at the end of its life cycle.

Secure data deletion techniques may include, among others:

- Secure deletion of information, obtainable through computer programs (such as "wiping programs" or "file shredder") which provide, once the user has deleted files from a disk unit or similar storage media with the normal tools provided by the various systems operations, to repeatedly write random sequences of "binary" digits (zero and one) in the empty areas of the disk (previously occupied by the deleted information) to minimize the chances of recover even through electronic tools for the analysis and recovery of data;
- "Low-level" formatting of hard disk-type devices (low-level formatting–LLF), where feasible, following the instructions provided by the device manufacturer and taking into account the possible technical consequences on it, up to its possible subsequent unusability;
- Demagnetization (degaussing) of memory devices based on magnetic or magneto-optical supports (hard disks, floppy disks, magnetic tapes on open reels or in cassettes), capable of guaranteeing the rapid deletion of information even on devices that are no longer functional to which the software deletion procedures may not be applicable (which require accessibility of the device by the system to which it is interconnected).

Safe device disposal techniques may include, but are not limited to:

- punching or mechanical deformation systems;
- physical destruction or disintegration (used for optical media such as CD-ROMs and DVDs);
- high intensity demagnetization.

Suppliers are required to deliver a certificate relating to the effective execution of the cancellation activity according to standard procedures such as ISO 27001 and ISO 27040.

MANAGEMENT OF REQUESTS FOR THE EXERCISE OF RIGHTS BY THE DATA SUBJECT

GENERAL PRINCIPLES

Any request by the Data Subject can be submitted through Digital Bros S.p.A. dedicated email addresses, dpo@digitalbros.com and privacy@digitalbros.com.

Data Subject can also submit their requests through other channels, namely:

- post office box (registered mail);
- contact form available on the Digital Bros S.p.A. websites.

In these cases, the corporate function / third party in charge of managing the channel used by the Data Subject must forward the request to the dedicated email address as soon as the request is received.

APPLICANT IDENTIFICATION

The first phase of the process involves the identification of the applicant; to this end, in fact, it is necessary that the Data Subject has indicated their Personal Data and contact details, as well as any information useful for their recognition.

Once the request has been received, with the support of the relative functions associated with the management of the request by the Data Subject, the Privacy Officer (assisted by the DPO) verifies (within 10 calendar days) the consistency and type of information possessed. If the Data Subject is not uniquely identifiable, they will be asked to complete the request with the information useful for his identification. The Data Subject identification is needed also in relation to the type of right exercised and, consequently, to any Personal Data that could be made available.

At the end of the identification process, the DPO will answer the request submitted by the Data Subject.

DATA COLLECTION AND VERIFICATION

Once the Data Subject identification has been completed, the DPO will start the collection of information concerning the Data Subject, which must be completed within 20 calendar days upon receiving the request. To this end, the competent functions for the collection/extraction of the necessary data will be involved.

In particular, the following function may be involved according to the request received:

- **Marketing** may be involved in requests concerning Customer data;

- **Administration** or **HR** may be involved in requests concerning Employees and self-employed personnel data, even at the end of the employment relationship.

Furthermore, the specific competent Functions, in the person of the respective Privacy Owner, must be involved for the collection of any information held by Third Parties that process data on behalf of Digital Bros S.p.A. and for the collection of any information stored in their archives.

The relevant functions contact the IT Systems Manager for data extraction.

Once the data has been collected and organized, the DPO, with the support of the Privacy Owners and the Privacy Officer, will verify the congruence of the data, the types and methods of treatment carried out, as well as the presence of the relative consents.

PREPARATION OF THE FEEDBACK

Once the data held by the Data Controller (and any third party Data Processors) have been collected and verified, the DPO and the relevant functions (i.e. the respective Privacy Owners) manage the request and draw up the response relating to the right exercised according to the methods described below within 30 (calendar) days upon receiving the request. This deadline may be extended up to 60 (calendar) days, taking into account the complexity and number of requests, without prejudice to the obligation to inform the Data Subject of this extension and the reasons for the delay within 30 (calendar) days of receiving the request. The DPO must approve the extension. If the request sent by the Data Subject copies the Supervisory Authority, the necessary communications will shall also copy the Supervisory Authority. If, on the other hand, it is the Supervisory Authority who requests the information, then all the necessary communications, following the analysis carried out, will be sent directly to the Supervisory Authority.

Based on the specific request received, the IT Systems Manager may possibly be involved in the management of the requests of the Data Subject (e.g. deletion of data from the systems, limitation of treatment, portability).

A. RIGHTS OF ACCESS

The Data Subject can obtain confirmation as to whether or not Personal Data concerning them is being processed. In this case, the Data Subject can access such Personal data and obtain, if requested, additional information regarding the purposes of the processing, the retention period (or, if this is not possible, the criteria used to define this period) or even the existence of an automated decision-making process, including profiling. Furthermore, the Data Subject may request a copy of the Personal Data being processed.

Based on the data collected, the DPO identifies, in collaboration with the relevant functions, the information to be provided to the Data Subject and prepares the response.

The response must be sent to the Data Subject even if the request to exercise the right of access cannot be accepted. In this case, the answer must contain the specific reasons and must be shared with the Privacy Officer.

B. RIGHT OF RECTIFICATION

The Data Subject can obtain (also following a request to exercise the right of access) the rectification of inaccurate information. The Data Subject also has the right to integrate any incomplete Personal Data, taking into account the purposes of the processing. In the event that a Data Subject requests the rectification and/or integration of their Personal Data, the following applies (by way of example but not limited to):

- customer data: the assessment of the possibility of carrying out the rectification, the operational management of the request and the preparation of the response is performed directly by the relevant function with the support of the DPO and the Information Systems Manager;
- data of employees and self-employed personnel: the evaluation of the possibility of carrying out the rectification, the operational management of the request and the preparation of the response is performed directly by the HR Administration function, with the support of the DPO and the Information Systems Manager.

In such context, it may be necessary to involve other corporate functions or Third Parties who manage additional physical archives or systems concerning the Data Subject request. Should any third party be involved, formal feedback on the successful execution of the request must be requested.

The response must be sent to the Data Subject even if the request to exercise the right of rectification cannot be accepted. In this case, the answer must contain the specific reasons and must be shared with the Privacy Officer.

C. RIGHT OF CANCELLATION

The exercise of this right provides for the cancellation of all Personal Data relating to the Data Subject. Following the collection and verification of the data held by the Data Controller (or any External Managers), the request will be processed if the:

- Personal Data is no longer necessary in relation to the purposes for which it was collected;
- Data Subject revokes the consent on which the treatment is based and there is no other legal basis for the treatment;

- Data Subject opposes the treatment pursuant to Article 21, paragraph 1, and there is no overriding legitimate reason to continue with the treatment;
- Data Subject opposes the processing for marketing purposes (pursuant to article 21, paragraph 2);
- Personal Data have been processed unlawfully;
- Personal Data must be deleted to fulfill a legal obligation under the Union or Member State law to which the Data Controller is subject.

In the event that a Data Subject requests the cancellation of their Personal Data, the following applies:

- Customer data: the assessment of the possibility of deleting, the operational management of the request and the preparation of the response is performed directly by the relevant function with the support of the DPO and the Information Systems Manager;
- Data of employees and self-employed personnel: the assessment of the possibility of deleting, the operational management of the request and the preparation of the response is performed directly by the HR Administration function, with the support of the DPO and the Information Systems Manager.

In such context, it may be necessary to involve other corporate functions or Third Parties who manage additional physical archives or systems concerning the Data Subject request. Should any third party be involved, formal feedback on the successful execution of the request must be requested.

The response must be sent to the Data Subject even if the request to exercise the right of cancellation cannot be accepted. In this case, the answer must contain the specific reasons and must be shared with the Privacy Officer.

D. RIGHT OF RESTRICTION OF PROCESSING

The exercise of this right provides for the limitation of use and processing of data to what is necessary for conservation purposes. This right can be exercised in some particular cases:

- if the Data Subject disputes the accuracy of the Personal Data, for the period necessary for the Data Controller to verify its accuracy;
- if, in the presence of unlawful processing, the Data Subject opposes the cancellation of Personal Data, requesting that the limitation of their use be ordered instead of cancellation;
- if the storage of the Personal Data by the Data Controller beyond its useful life in needed to safeguard the Data Subject possibility to ascertain, exercise or defend a right in court;

- if in the event of opposition to the processing of Personal Data, the checks necessary to determine the prevalence of the legitimate reasons of the Data Controller or the rights of the Data Subject are pending.

In such cases, the data must be processed only for the purpose of their conservation, unless the Data Subject consents to the processing for different purposes, or the processing is necessary for the exercise or defense of a right in court, for the protection of the rights of another natural or legal person or for reasons of interest.

If the request of the Data Subject cannot be processed (pursuant to the provisions of the GDPR), the DPO will inform the Data Subject of the impossibility of following up on his request: in this case, the response must contain the specific reasons and must be shared with the Privacy Officer.

If, on the other hand, it should be necessary to follow up on the request, the DPO will involve the relevant functions, through the related Privacy Owners, in order to:

- mark and make the data inaccessible from all corporate systems, thus blocking any further processing;
- collect all data in paper format and organize them in a dedicated section;
- inform any External Data Manager of the Personal Data whose limited processing has been requested and receive feedback on the successful limitation.

The limited data can then be unlocked (thus resuming the processing) only with the express consent of the Data Subject, or they can be processed - without consent - only and exclusively for the assessment, exercise or defense of a right in court or to protect the rights of another natural or legal person.

At the end of the activities, the DPO will inform the Data Subject of the outcome of the request. Furthermore, the Data Subject who has obtained the limitation of the treatment is informed before the said limitation is revoked.

E. RIGHT TO DATA PORTABILITY

The Data Subject may request their Personal Data in a structured format if:

- the treatment is based on consent or on a contract;
- the processing is carried out by automated means.

All requests received must be handled by the DPO who, with the support of the relevant functions, identifies among the information collected which of the Personal Data are portable.

The relevant function, with the support of the Information Systems Manager if needed, provides the DPO with the extraction of data in a structured format (with particular reference to the data provided by

the same Data Subject), exclusively in the case in which Personal Data for which this right is applicable have been identified.

If the Data Subject expressly requests the Personal Data to be transferred to another Data Controller, the DPO, with the support of the relevant functions, will contact the Data Controller requested to define the methods of transmission. In this case, the request can only be processed if technically possible.

At the end of the activities, the DPO communicates the outcome of the request to the Data Subject, providing the Data Subject or the Data Controller requested the documentation produced according to what was agreed on.

The response must be sent to the Data Subject even if the request to exercise the right to data portability cannot be accepted. In this case, the answer must contain the specific reasons and must be shared with the Privacy Officer.

F. RIGHT TO OBJECT

The Data Subject may object at any time to the processing of their Personal Data, including the processing connected to reasons of public interest or implemented for the pursuit of legitimate interests of the Data Controller. All requests received must be handled by the DPO. Once the request has been received and the data possessed has been collected and verified, the DPO will proceed to verify the existence of legitimate reasons to continue with the processing pursuant to the provisions of the GDPR. If so, the DPO informs the Data Subject of the impossibility of following up on their request, specifying the reasons in detail.

Otherwise, the DPO, with the support of the relevant functions and the Information Systems Manager, identifies among the information collected which are the Personal Data for which the right to object can be exercised and proceeds with the Data Subject request.

The Privacy Owners of the specific relevant functions must be involved for the collection of any information held by Third Parties who process data on behalf of Digital Bros S.p.A. and for the collection of any information stored in its archives.

The Data Subject can also oppose the processing of data for commercial purposes (such as direct marketing and profiling); in these cases, the processing of Personal Data will be terminated. To this end, for certain types of activities and treatments (e.g. newsletters) Digital Bros S.p.A. prepares specific automated systems for withdrawing consent (e.g. newsletter **unsubscribe button**).

At the end of the aforementioned activities, the DPO will inform the Data Subject of the outcome of their request.

FILING OF REQUESTS

Requests to exercise rights by Data Subjects are mapped in a document based on the Model - Management of Data Subjects requests.