Policy [5.1.1]

Data Protection Policy

Object	*This policy is a set of working instructions, relevant to how Flowbird stores personal data, that enables data subjects to either update their own data or to provide Flowbird with details of changes to their data.*
Stakeholders	Permanent and temporary Employees/Staff and subcontractors.
Document Classification	**Public**
Communicability	Public

Scope of application:	This policy covers all Flowbird information systems.	*Version :*	1.5
Date of first application:	2018-05-25	*Approved by:*	Flowbird Executive Committee
Issued by:	InfoSec Team	*Policy Managed by:*	Flowbird DPO

Version	Date dd/mm/yyyy	Modification
1.0	25/05/2018	Initial version
1.1	22/06/2018	Change the Communicability to Public
1.2	29/11/2018	Integration of VE remarks and validation of VE's suggestions
1.3	03/12/2018	Clarification in §4.1.9. Manage the complete data lifecycle in §4.5. Remove the "§9. Disposal of Data" which is included in §4.5
1.4	06/04/2021	Clarification on DPO role and DPO name update
1.5	14/01/2022	Update relocation of headquarters and policy storage
1.6	06/04/2023	Update relocation of headquarters

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group

1. Introduction

1.1. Background to the General Data Protection Regulation ('GDPR')

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

1.2. Definitions used by Flowbird (drawn from the GDPR)

Material scope (Article 2) – the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) – the GDPR will apply to all controllers that are established in the EU (European Union) who process the personal data of data subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process personal data in order to offer goods and services, or monitor the behavior of data subjects who are resident in the EU.

1.3. Article 4 definitions

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with Supervisory Authorities (SAs).

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behavior. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the SA where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – the GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Recipient - a natural or legal person, public authority, agency or other body, to which the personal data is disclosed (whether a 3rd party or not).

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group

2. Policy statement

2.1. The Top Management/Board of Directors and management of Flowbird, located at 2 T Rue du Château 92200 Neuilly-sur-Seine, France, are committed to compliance with all relevant EU and Member State laws in respect of personal data, and the protection of the “rights and freedoms” of individuals whose information Flowbird collects and processes in accordance with the General Data Protection Regulation (GDPR).

2.2. Compliance with the GDPR is described by this policy and other relevant policies such as the Information Systems Security Policy, along with connected processes and procedures.[1]

2.3. The GDPR and this policy apply to all of Flowbird’s personal data processing functions, including those performed on personal data of customers, clients, employees, suppliers and partners, and any other personal data the organisation processes from any source.

2.4. Flowbird has established objectives for data protection and privacy, which are in this Policy and GDPR Objectives Record.

2.5. Data Protection Officer/Data Processing Owner is responsible for reviewing the register[2] of processing annually in the light of any changes to Flowbird’s activities and to any additional requirements identified by means of risk assessments. This register needs to be available on the SA’s request.

2.6. This policy applies to all Employees/Staff and interested parties of Flowbird such as outsourced suppliers. Any breach of the GDPR or this Policy will be dealt with under Flowbird’s disciplinary sanctions and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

2.7. Partners and any third parties working with or for Flowbird, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by Flowbird without having first entered into a data confidentiality agreement, which imposes on the third party obligations no less onerous than those to which Flowbird is committed, and which gives Flowbird the right to audit compliance with the agreement.

3. Responsibilities and roles under the General Data Protection Regulation

[1] Policy [5.1.1] - Information System Security Policy
[2] processing register GDPR

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group

3.1. Flowbird is a data controller and data processor under the GDPR.

3.2. Top Management and all those in managerial or supervisory roles throughout Flowbird are responsible for developing and encouraging good information handling practices within Flowbird; responsibilities are set out in individual job descriptions.

3.3. Data Protection Officer, a role specified in the GDPR, is a member of the senior management team, is accountable to Top Management/Board of Directors of Flowbird for the management of personal data within Flowbird and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

3.3.1. development and implementation of the GDPR as required by this policy; and

3.3.2. security and risk management in relation to compliance with the policy.

3.4. Data Protection Officer, who Top Management/Board of Directors considers to be suitably qualified and experienced, has been appointed to take responsibility for Flowbird's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that Flowbird complies with the GDPR, as do Executives (generic/line) in respect of data processing that takes place within their area of responsibility.

3.5. The Data Protection Officer / Data Processing Owner has specific responsibilities in respect of procedures such as the Data Subject Access Request (DSAR) Procedure and are the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance.

3.6. Compliance with data protection legislation is the responsibility of all Employees/Staff of Flowbird who process personal data.

3.7. Flowbird's Training Policy sets out specific training and awareness requirements in relation to specific roles and Employees/Staff of Flowbird generally.

3.8. Employees/Staff of Flowbird are responsible for ensuring that any personal data about them and supplied by them to Flowbird is accurate and up-to-date.

4. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. Flowbird's policies and guidelines are designed to ensure compliance with the principles.

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group

4.1. Personal data must be processed lawfully, fairly and transparently

Lawfully – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent [for further details, see Article #6 & #9].
Processing will only be lawful if one of the following conditions is met:

1. Data Subject gives Consent for one or more specific purposes
   OR any of the below:
2. Processing is necessary to meet contractual obligations entered into by the Data Subject
   e.g. employee – bank details – payroll to get salary
3. Processing is necessary to comply with legal obligations of the Controller
   e.g. payment records for accounting and/or tax purposes
4. Processing is necessary to protect the vital interests of the Data Subject
   e.g. blood group
5. Processing is necessary for tasks in the public interest or exercise of authority vested in the Controller.. government identifies such.
   e.g. council tax
6. processing is for the purposes of legitimate interests pursued by the Controller
   e.g. finance company who is unable to locate a customer who has fallen into arrears on a purchase agreement and moved houses without notification – share Personal Data with a Debt Collection Agency but only info which helps the debt collector to collect.

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects (in which case the data controller must explain at the point of collection) or from other sources.
The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparency' requirement.
Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language: be transparent about how you intend to use data (legitimate grounds for collecting and using), handle data in ways data subjects would reasonably expect and not use data in ways that have unjustified adverse effects on data subjects.
Flowbird's Privacy Notice procedure is set out in a Guideline[3] and the Privacy Notice is recorded.
The specific information that must be provided to the data subject must, as a minimum, include:

[3] GUIDELINES [18.1.4] - How to inform individuals whose data is collected

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group

4.1.1. the identity and the contact details of the controller and, if any, of the controller's representative;

4.1.2. the contact details of the Data Protection Officer;

4.1.3. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

4.1.4. the period for which the personal data will be stored;

4.1.5. the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;

4.1.6. the categories of personal data concerned;

4.1.7. the recipients or categories of recipients of the personal data, where applicable;

4.1.8. where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;

4.1.9. any further information necessary to guarantee fair processing as of Article 13.2.

4.2. Purpose Limitation: personal data can only be collected for specific, explicit and legitimate purposes.

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the SA as part of Flowbird's GDPR register of processing. The shared drive ISMS[4] portal sets out the relevant procedures.
Specific: purpose clearly stated upon collection of data; any change in purpose where Flowbird must ensure that if it wishes to use or disclose data for any purpose other than originally specified, the new use is compatible with the originally specified purpose; disclosure: purpose for which it will be used after disclosure (if no mentioning of disclosure originally, needs additional consent or any other lawful basis for disclosure), make data subject aware of disclosure
Explicit: data subject needs to be able to consent / object to some processing activities and not to others (granular consent management), anything that is vague and uncertain fails this point such as 'associated purposes' or 'to meet business requirements'.
Legitimate (incl. Recitals 47 - 50): careful assessment required regarding:

- processing of data for purpose of ***preventing fraud***
- processing of data for ***direct marketing***
- internal processing (incl. to 3rd countries)
- ensuring ***network security***
- purposes directly related to the purpose for which data was collected
- data about criminal acts

[4] ISMS shared drive

4.3. Data Minimization: Personal data must be adequate, relevant and limited to what is necessary for processing

Adequate (nothing less): just enough for the purpose

Relevant: to the purpose for which Flowbird collects the data (USA's 'just in case' approach doesn't work anymore)

Limited (nothing more): exactly the amount what is required to the extent of Flowbird's purposes, nothing more.

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group

4.3.1. The Data Protection Officer / Data Processing Owner is responsible for ensuring that Flowbird does not collect information that is not strictly necessary for the purpose for which it is obtained through the risk assessment procedure[5].

4.3.2. All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to privacy statement and be approved by the Data Protection Officer.

4.3.3. The Data Protection Officer / Data Processing Owner will ensure that, on an annual basis all data collection methods are reviewed by either internal audit or external experts to ensure that collected data continues to be adequate, relevant and limited (not excessive[6]).

4.4. Data Integrity: personal data must be accurate and kept up to date with every reasonable effort to erase or rectify without delay

4.4.1. Data that is stored by the data controller must be reviewed and updated as necessary, and its source needs to be clear. No data should be kept unless it is reasonable to assume that it is accurate.

4.4.2. The Data Protection Officer is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

4.4.3. It is also the responsibility of the data subject to ensure that data held by Flowbird is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

4.4.4. Employees/Staff/customers/others should be required to notify Flowbird of any changes in circumstance to enable personal records to be updated accordingly. Instructions for updating records are contained in dedicated documents. It is the responsibility of Flowbird to ensure that any notification regarding change of circumstances is recorded and acted upon.

4.4.5. The Data Protection Officer / Data Processing Owner is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

4.5. Data Retention / Storage Limitation

[5] Procedure [1] - Risk Assessment Procedure
[6] GUIDELINES [18.1.4] - How to comply with GDPR in 6 steps

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group

4.5.1. Flowbird shall not keep personal data in a form that permits identification of data subjects for a longer period than is necessary, in relation to the purpose(s) for which the data was originally collected.

4.5.2. Flowbird may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

4.5.3. The retention period for each category of personal data will be set out in the Retention of Records Procedure along with the criteria used to determine this period including any statutory obligations Flowbird has to retain the data.

4.5.4. Flowbird's data retention and data disposal procedures (Storage Removal Procedure) will apply in all cases.

4.5.5. Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the secure disposal procedure.

4.5.6. On at least an annual basis, the Data Protection Officer / Data Processing Owner will review the retention dates of all the personal data processed by Flowbird, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with a Secure Disposal of Storage Media Procedure.

* Attention: each purpose of collection could have a deferring retention requirement**.**

Right to rectification The Data Protection Officer / Data Processing Owner is responsible for responding to requests for rectification from data subjects within one month. This can be extended to a further two months for complex requests. If Flowbird decides not to comply with the request, the Data Protection Officer / Data Processing Owner must respond to the data subject to explain its reasoning and inform them of their right to complain to the SA and seek judicial remedy.

4.5.7 The Data Protection Officer / Data Processing Owner is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

4.5.8 Personal data is to be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which data are processed.

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group

4.5.9. Where personal data is retained beyond the processing date, it will be minimised / encrypted / pseudonymised in order to protect the identity of the data subject in the event of a data breach[7].

4.5.10. Personal data will be retained in line with the Retention of Records Procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

4.5.11. The Data Protection Officer / Data Processing Owner must specifically approve any data retention that exceeds the retention periods defined in Retention of Records Procedure, and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

4.6. Personal data must be processed in a manner that ensures the *appropriate security* of personal data (refer to GDPR articles 24 & 32)

The Data Protection Officer / Data Processing Owner will carry out a risk assessment[8] taking into account all the circumstances of Flowbird's controlling or processing operations (unauthorized or unlawful processing).
In determining appropriateness, the Data Protection Officer / Data Processing Owner should also consider the extent of accidental loss / damage / destruction / that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on Flowbird itself, and any likely reputational damage including the possible loss of customer trust.

When assessing appropriate technical measures, the Data Protection Officer / Data Processing Owner will consider the following[9]:

- Password protection;
- Automatic locking of idle terminals;
- Encrypt sensitive data, especially on potentially lossable hardware;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the organisations premises such as laptops;
- Security of local and wide area networks;
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate international security standards relevant to Flowbird.

When assessing appropriate organisational measures the Data Protection Officer / Data Processing Owner will consider the following:

- The appropriate training levels throughout Flowbird;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;

[7] Procedure [16.1.1] - Security incident management procedure
[8] Procedure [1] - Risk Assessment Procedure
[9] Baseline [12.1] - Operations security

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group

    - Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices (BYOD) being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.
Flowbird's compliance with the 6th principle (Confidentiality - Integrity - Availability) is contained in its Information Security Management processes, which have been developed in line with ISO/IEC 27001:2013 and the information systems security policy[10].

- **Confidentiality**: making sure that any of those with authorization are able to access the data. Regulators will look at: what types of controls you put in place to identify: who can authorize access to data and the registration process for access to that data.
- **Integrity**: refers back to Principle 4.
  Regulators will look at: what types of controls you put in place to protect data from corruption; what types of logs are in place to track who has had access to data and what changes might have been made to that data.
- **Availability**: the way in which information is protected from unauthorized disclosure of data i.e. the technical controls put in place against hacking.

4.7. The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.
Flowbird will demonstrate compliance with the data protection principles by implementing data protection policies[11], adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, Data Protection Impact Assessments (DPIAs), personal data breach (PDB) notification procedures and incident response plans.

[10] Policy [5.1.1] - Information Systems Security Policy
[11] ISMS shared drive

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group

5. Data subjects' rights (Article 15 - 21)

5.1. Data subjects have the following rights regarding data processing, and the data that is recorded about them:

5.1.1.Right of Access by Data Subject (Article 15): A request made by or on behalf of the data subject for information which he / she is entitled, i.e. data subject can inquire Flowbird what he/she is doing with his data at any point in time::

- Purpose(s) of processing (lawfulness)
- Categories of personal data
- Recipients to whom personal data have been or will be disclosed
- Retention: period for which personal data will be stored
- Right to rectification (Article 16) – erasure (Article 17) – restriction (Article 18) – objection (Article 21)
- Right to lodge a complaint with a SA (Article 77)
- Where personal data is not collected from data subjects, any available information as to their source

Flowbird has 1 month (with a possible 1 month of extension for complex requests) to respond to the data subject.

DSAR management

Stages of DSAR management:

Stage 1 Recognize a DSAR	Stage 2 Validate DSAR	Stage 3 Redact	Stage 4 Maintain records
• Written or oral • Phone, social media • Quick funneling into a format route	Identification: • Photo ID • Address DSAR on behalf of ..: • 3rd parties • Children	• Exemptions from disclosure • Remove any 3rd party info DS is not entitled to access	• Track progress • Keep track of time (1+1 month)

Types of DSARs:

1. Simple DSAR
    - single location for data

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group

- does not involve release of 3rd party data *
- DPO may be consulted to validate disclosure, and identify what can be disclosed and what should be withheld (i.e. redacted) **

2. Complex DSAR
   - several requests from same DS
   - multiple location for data
   - involves release of 3rd party data *
   - DPO or legal advisor must be consulted to validate disclosure, and identify what can be disclosed and what should be withheld (i.e. redacted) **
   - release of contentious info

NB: archived data is subject to DSARs and exercise of all data subjects' rights.

Stage 3 in more details

* Disclosure of 3rd party data in a DSAR:

- Data should not be disclosed of 3rd party without 3rd party Consent!
- If Consent cannot be obtained, the following must be taken into account:
  - duty of Confidentiality to 3rd party
  - steps taken to seek 3rd party Consent
  - whether 3rd party is capable of giving Consent
  - any express refusal of Consent

** Withheld (redacted) data

- Disclosure should clearly state that some information was redacted and why.

Stage 4 – Maintain Records of DSAR in more details

Controller must maintain a centralized record of all DSARs containing information such as:

1. Date and time of receipt of DSAR
2. Details of DSAR
3. Confirmation of identification
4. Date and time of response to DSAR
5. Issues or concerns

5.1.2 Right to Rectification (Article 16)

Data subjects shall have the right to the rectification of inaccurate PD:

- right to have incomplete data completed or inaccurate data corrected
- including by means of a supplementary statement
- If Controller has disclosed PD in question to 3rd parties, Controller must inform them of rectification where possible

Best practice: a Customer Portal which enables data subjects to address Flowbird re. any GDPR-related issue.

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group

5.1.3 Right to Erasure (commonly known as right to be forgotten) [Article 17]

Data subjects have the right to the erasure of personal data where one of the following grounds applies (not an absolute right, applies only in specific circumstances):

- Data are no longer necessary in relation to the purposes for which they were collected or otherwise processed
- Data subject withdraws Consent on which the processing is based and where there is no other legal ground for the processing
- Data subject objects to the processing and there are no overriding legitimate grounds for the processing
- Processing is unlawful
- Personal data have to be erased to comply with a legal obligation
- Personal data have been collected for Information Society Services

! IF deletion is not possible >> **ANONYMIZE** therefore data subject is unrecognizable.

Exceptions - Controller may refuse a request to erase personal data:

- where Controller needs to comply with a legal obligation (tax: invoice retention)
- for vital interests of tasks carried out in public interest
- when archiving in relation to public interest – scientific/historic purpose – statistical research
- required for the establishment – exercise – defense of legal claims.

Where personal data was shared with 3rd party, Controller must:

- inform 3rd party processing personal data unless it involves ***disproportionate effort*** to do so (erase any links or copies of personal data)
- take into consideration the technology and means available, and review circumstances on a regular basis (if not now, justify and review again at a later time)
- Exception: requirements in respect of right of erasure do not apply where processing is necessary for 'exercising right of freedom of expression and information'

5.1.4 Right to restriction of processing (Article 18)

Data subject shall have the right to restriction of processing where one of the following applies:

- Accuracy of personal data is contested by data subject (for a period that enables Flowbird to verify accuracy)
- Processing is unlawful, and data subject opposes the erasure of personal data and requests the restriction of their use instead. [e.g. payment data for later reference requests]
- Controller no longer needs the personal data for the purposes of original processing but data is required by data subject for the establishment – exercise – defense of legal claims.
- Data subject has objected to processing pending verification whether legitimate grounds of Controller override those of data subject.

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group

Controller may only resume processing of restricted personal data if:

- Consent is given by data subject
- Processing is required in relation to legal matters or to protect rights of another data subject
- Controller must inform data subjects when he decides to lift a restriction on processing.

5.1.5 Right to Data Portability (Article 20)

Data subject has the right to have personal data transmitted to another Controller where technically feasible.

Right to Data Portability only applies where:

1. data subject provided the data, and
2. data subject gave Consent to the processing or the processing is necessary to fulfil a contract, and
3. data is processed by automated means,

- Flowbird (as Controller) must provide data subject with a copy of personal data in a structured – commonly used – machine-readable format;
- Flowbird must not hinder the transmission of personal data to a new Controller.

E.g. cell phones. Carry number over from one service provider to another.

5.1.6 Right to object

Data subject shall have the right to object to:

- Processing for a task in the public interest (Controller is not required to comply) as per Recitals 69 & 70;
- Processing based on legitimate interests:
  - processing of personal data for direct marketing
  - processing of personal data by automated decision making or profiling (Recitals 71 & 72)
  - processing for scientific research (Recitals 69 & 70) or historical purposes

Right to object is:

1. not to be subject to a decision based solely on automated processing (incl. profiling) which produces legal effects concerning data subjects:
   - Does not apply if:
     - necessary for entering into or performance of a contract between Controller & data subject
     - authorized by Member State law which includes measures to safeguard data subjects' rights
     - is based on explicit Consent

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group

- Controller must ensure that data subjects are able to:
  - obtain human intervention, and
  - express their point of view, and
  - obtain an explanation of decision and also challenge it!

2. not to be based on special categories of data (Article 9) unless:
   - data subject has given explicit Consent (9.2.a), or
   - processing is necessary for reasons of substantial public interest (9.2.g), AND
   - suitable measures to protect rights and freedoms are in place

* If processing activities take place online, Controller must offer a way for data subjects to object online.

Exceptions

Controller must demonstrate compelling legitimate grounds for:

1. the processing that override the interests – rights – freedoms of the data subject, or
2. the establishment – exercise – defense of legal claims.

NB: Controller must inform data subject of their right to object:

1. 'at the point of first communication' (upon registration) AND
2. in the Privacy Notice

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group

5.1.7. To prevent processing likely to cause damage or distress.

5.1.8. To prevent processing for purposes of direct marketing.

5.1.9. To be informed about the mechanics of automated decision-taking process that will significantly affect them.

5.1.10. To not have significant decisions that will affect them taken solely by automated process.

5.1.11. To sue for compensation if they suffer damage by any contravention of the GDPR.

5.1.12. To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.

5.1.13. To request the SA to assess whether any provision of the GDPR has been contravened.

5.1.14. To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.

5.1.15 To object to any automated profiling that is occurring without consent.

5.2. Flowbird ensures that data subjects may exercise these rights:

5.2.1. Data subjects may make data access requests as described in DSAR Procedure; this procedure also describes how Flowbird will ensure that its response to the data access request complies with the requirements of the GDPR.

5.2.2. Data subjects have the right to complain to Flowbird related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Complaints Procedure.

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group

6. Consent

6.1. Flowbird understands ‘consent’ to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject’s wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time, and it must be as easy to withdraw consent as give it (e.g. register online but unsubscribe via postal letter is unacceptable).

6.2. Flowbird understands ‘consent’ to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

6.3. There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication (e.g. a box ticked in by default). The Controller must be able to demonstrate that consent was obtained for the processing operation.

6.4. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.[12][13]

6.5. In most instances, consent to process personal and sensitive data is obtained routinely by Flowbird using standard consent documents e.g. when a new client signs a contract, or during induction for participants on programmes.

6.6. Where Flowbird provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 16 (unless the Member State has made provision for a lower age limit, which may be no lower than 13).

6.7 Consent should be the last resort from a Controller’s perspective based on which it collects personal data as it can be withdrawn at any time by the data subjects which does not absolve Flowbird from the original contractual / legal obligations; merely hinders Flowbird in processing the data in the particular way the consent was given. Therefore, any of the five conditions for lawful processing other than consent as per Article 6 is more favorable.

[12] GUIDELINES [18.1.4] - How to request the user consent
[13] GUIDELINES [18.1.4] - How to get employee's consent to use his personal data

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group

7. Security of data

7.1. All Employees/Staff are responsible for ensuring that any personal data that Flowbird holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Flowbird to receive that information and has entered into a confidentiality agreement[14].

7.2. All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. All personal data should be treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with corporate requirements in the Access Control Policy; and/or
- stored on (removable) computer media which are encrypted in line with Secure Disposal of Storage Media[15].

[14] Flowbird's Non DIsclosure Agreement
[15] Baseline [12.1] - Operations security

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group

7.3. Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees/Staff of Flowbird. All Employees/Staff are required to enter into an Acceptable Use Agreement before they are given access to organisational information of any sort, which details rules on screen time-outs.

7.4. Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit written authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with the Manual Records Management Procedure.

7.5. Personal data may only be deleted or disposed of in line with the Retention of Records Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required by disposal procedure.

7.6. Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site with reference to remote and flexible working arrangements.

8. Disclosure of data

8.1. Flowbird must ensure that personal data is not disclosed to unauthorised third parties which include family members and friends. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of Flowbird's business. The GDPR permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- to safeguard national security;
- to prevent or detect crime including the apprehension or prosecution of offenders;
- assessment or collection of tax duty;
- to discharge regulatory functions (including health, safety and welfare of persons at work);
- to prevent serious harm to a third party; and
- to protect the vital interests of the individual, this refers to life and death situations.

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group

8.2. All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer / Data Processing Owner.

9. Data transfers

9.1. All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

9.1.1. An adequacy decision (Article 45)

The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances no authorisation is required.
Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision.
A list of countries that currently satisfy the adequacy requirements of the Commission are published in the Official Journal of the European Union.
http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

9.1.2. Transfers of data to the United States

We have implemented measures to protect personal data, including by using the European Commission's Standard Contractual Clauses for transfers of personal information between our group companies and between us and our third-party providers. Ther clauses require all recipients to protect all personal information that they process originating from the EEA in accordance with European data protection laws and regulations. We have implemented similar appropriate safeguards with our third-party service providers, subsidiaries and partners.

Appropriate Safeguards put in place by exporting Data Controller (Article 46)
In making an assessment of adequacy, the exporting controller should take account of the following factors:

- the nature of the information being transferred;
- the country or territory of the origin and final destination of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations.

9.1.3. Binding Corporate Rules (Article 47: BCR)

Flowbird may adopt approved binding corporate rules for the transfer of data outside the EU. This requires submission to the relevant SA for approval of the rules that Flowbird is seeking to rely upon.

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group

How to get authorization for BCRs:

1. Create your BCR valid for your own specific circumstances
2. Obtain approval from SA
   - select a SA to be the Lead SA
   - submit BCR Authorization Request using the Standard Application Form (BCR Checklist)
   - if Lead SA is satisfied as to the adequacy of the safeguards put in place in your BCR, that decision is binding across the other SAs in EU

NB (1): Member States may have additional requirements.
NB (2): Any change to BCR requires a re-application!

9.1.4. Model contract clauses

Flowbird may adopt approved model contract clauses for the transfer of data outside of the EEA. If Flowbird adopts the [model contract clauses approved by the relevant SA] there is an automatic recognition of adequacy. Link to current template of Model Contract Clause.

9.1.5. Exceptions (Article 49: Derogations)

In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules and/or model contract clauses, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

10. Information asset register/data inventory

10.1. Flowbird has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project. Flowbird's data inventory and data flow determines[16]:

- business processes that use personal data;
- source of personal data;
- volume of data subjects;
- description of each item of personal data;
- processing activity;

[16] The Flowbird Processings Register

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group

    - maintains the inventory of data categories of personal data processed;
- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of Flowbird throughout the data flow;
- key systems and repositories;
- any data transfers (international transfers); and
- all retention and disposal requirements.

10.2. Flowbird is aware of any risks associated with the processing of particular types of personal data.

10.2.1. Flowbird assesses the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs) are carried out in relation to the processing of personal data by Flowbird, and in relation to processing undertaken by other organisations on behalf of Flowbird.

10.2.2. Flowbird shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

10.2.3. Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Flowbird shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

10.2.4. Where, as a result of a DPIA, it is clear that Flowbird is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not Flowbird may proceed must be escalated for review to the Data Protection Officer/Data Processing Owner.

10.2.5. The Data Protection Officer / Data Processing Owner shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the SA.

10.2.6. Appropriate controls will be selected primarily from Annex A of ISO 27001, ISO 27017, ISO 27018, etc., as appropriate and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to Flowbird documented risk acceptance criteria and the requirements of the GDPR.

11. Document Owner and Approval

The Data Protection Officer is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of staff on the ISMS shared drive

This policy was approved by the Top Management/Board of Directors on ../../…. and is issued on a version controlled basis under the signature of the Chief Executive Officer (CEO).

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group

Signature: Date:

Flowbird · head office: 2 ter rue du château, 92200 Neuilly-sur-Seine - France
Tel: +33 (0)1 58 09 81 10 - www.flowbird.group