BRACCO

LIFE FROM INSIDE

data protection program

BRACCO

LIFE FROM INSIDE

data protection program

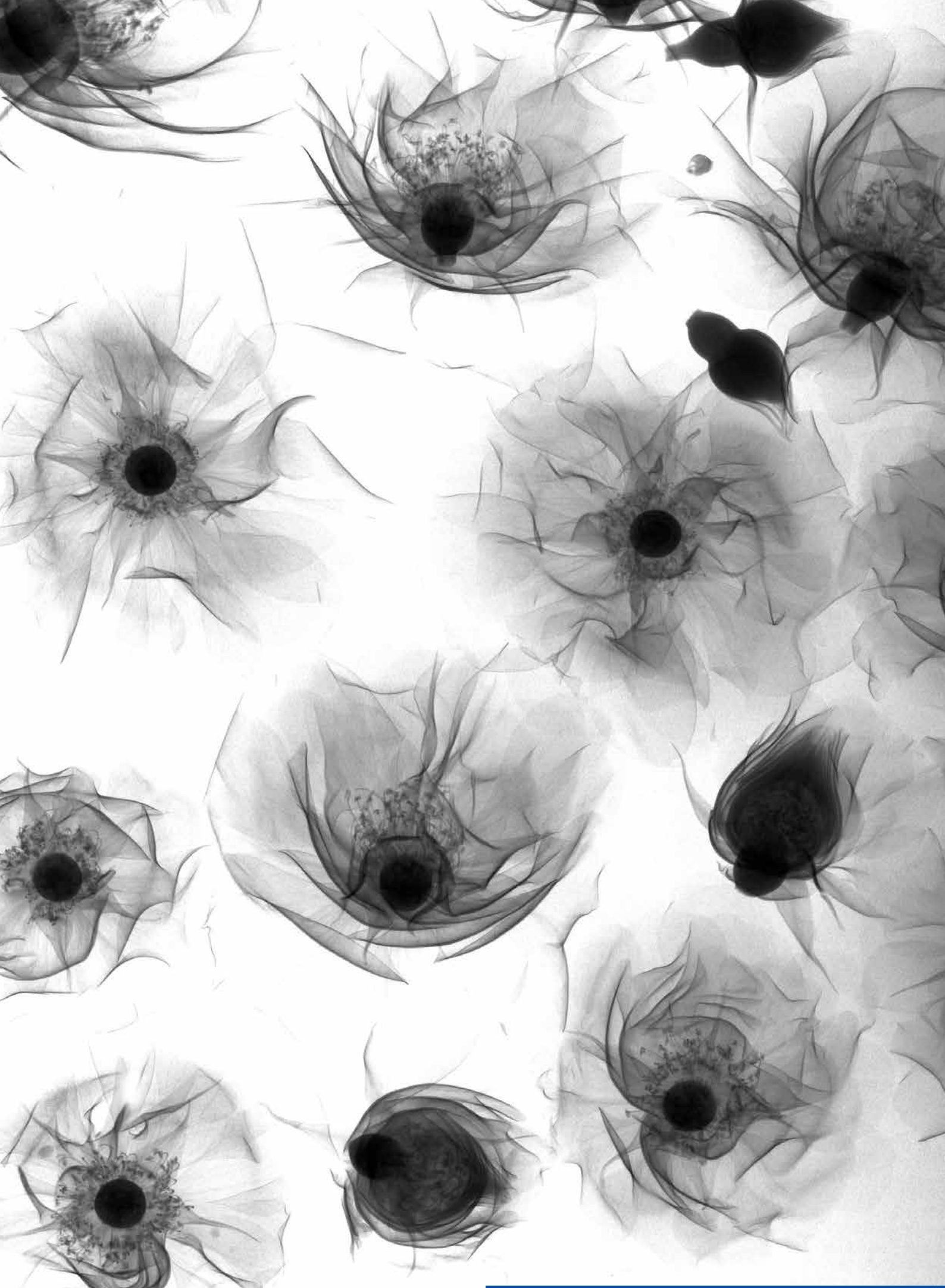
The Bracco Group Data Protection Policy outlines a set of principles, rights, duties and responsibilities that all recipients must comply with.

The Bracco Group implements requirements for the protection and safeguarding of personal data through the enforcement of suitable organizational measures.

Each company of the Bracco Group shall implement the above principles, adopt suitable technical measures, including without limitation IT security measures pursuant to applicable policies and can define additional rules to adapt the Data Protection Program to its needs, the local social context and legislative and regulatory framework. In any case, any additional obligations set forth shall not override the principles established by law and this document.

“We believe that any person who works in our Group **shall adhere to the highest international privacy standards** in all our business dealings and relationships, wherever we operate, with the aim to implement and enforce all the effective systems useful to guarantee **the protection of personal data.**”

Diana Bracco
Chairwoman and CEO of the Bracco Group



Bracco is committed to **protect personal data of any data subject,** including the personal data of **customers, employees, participants in clinical studies and business partners,** in accordance with the **highest standards** and **data protection laws and regulations** applicable in the countries where we operate.

Fulvio Renoldi Bracco
Vice Chairman and CEO of Bracco Imaging SpA

1 PURPOSE

This document provides guidance (general principles) to Companies of the Bracco Group to follow when processing Personal Data, at global and local levels, to ensure compliance with applicable laws and regulations, and to enable the uniform management of activities involving the Processing of Personal Data across the Bracco Group.

This Program implements the Bracco Group Code of Ethics with reference to personal data protection and should be read in conjunction with:
(i) the Glossary (which contains the definitions of the relevant terms and abbreviations);
(ii) the Data Protection Guideline;
and (iii) applicable Data Protection local SOPs (indeed, in order to deploy the principles and Procedures set out in this Program and in the Data Protection Guideline, each Company of the Bracco Group should evaluate if a local SOP needs to be adopted, based on the templates attached to the Data Protection Guideline).
The Bracco Data Protection Program is available on the Bracco Intranet, in order to inform Personnel about the importance of Personal Data protection, and on the Group website, in order to explain to third parties the measures taken by the Bracco Group to fulfil its commitment to protect privacy and Personal Data.

2 SCOPE

Companies of the Bracco Group shall comply with this Program when they collect, use, retain or disclose Personal Data of any Data Subject, including employees, HCPs, patients in clinical studies, customers, or business partners, whether they conduct such processing activities on their own behalf (i.e. act as Data Controller) or on behalf of a third party (i.e. act as Data Processor). It must also be followed when Companies of the Bracco Group acting as Data Controllers appoint Data Processors to conduct activities involving Personal Data Processing on their behalf.

In the field of data protection, Centro Diagnostico Italiano implements its own policies and procedures in view of its specific business.

In the event of conflict or inconsistency between applicable legal and regulatory provisions and the provisions of this Program, applicable laws and regulations shall prevail. Companies of the Bracco Group shall notify without undue delay the Group DPO when they identify a legal or regulatory provision that prevents them from complying with the principles of this Program (unless such notification is prohibited by applicable law or by the competent supervisory authority).

If applicable data protection laws or regulations are less strict than this Program, the general principles stated herein shall prevail.

This Program applies to all activities involving Processing of Personal Data that fall within the scope of the Data Protection Guideline and relevant Procedures and local SOPs.

3 INVOLVED FUNCTIONS

Group Privacy Committee; Group Data Protection Officer; Local Data Protection Officers or Privacy Focal Points; Processing Owners; Delegates of Processing Owners; Information Technology Services (ITS) Department.

4 RESPONSIBILITIES

It is the responsibility of all functions and directors, employees (at all levels), collaborators as well as everyone working for or in the name and on behalf of the Bracco Group involved in Processing activities to follow this Program, the Data Protection Guideline and relevant local SOPs.

Allegations of breaches of this Program, the Data Protection Global Guidelines or SOPs, or applicable laws and regulations, may be sent to the Group DPO (dpo@bracco.com) and/or through the whistleblowing channel

email: corporateIA@bracco.com

IT tool: http://bracco.mrowhistle.com

Hotline: tel. +39 02 21772607.

Any employee or agent sending a notice alleging that data protection rules have been breached will be protected from any harassment, retaliation and discrimination, and his or her identity will be kept confidential.

Failure to comply with this Data Protection Program, the Data Protection Guideline and Procedures, with local SOPs, and with applicable laws and regulations could amount to a misconduct. Companies of the Bracco Group have the right to take adequate disciplinary measures and request appropriate remedies against any employee who intentionally or negligently breaches applicable data protection standards.

5

GENERAL PRINCIPLES

Companies of the Bracco Group must comply with the following general principles whenever they collect, process, store, transfer or disclose Personal Data on their own behalf (i.e. as Data Controllers) or on behalf of a third party (i.e. as Data Processors). They shall retain all necessary documentation to demonstrate compliance with the principles stated herein and with any applicable laws or regulations.

5.1. LAWFULNESS, FAIRNESS AND TRANSPARENCY OF THE PROCESSING

Personal Data must be collected and processed lawfully, fairly and in a transparent manner.

Companies of the Bracco Group acting as Data Controllers must have a lawful basis to process Personal Data. When the lawful basis for a Processing activity is 'legitimate interests', a Legitimate Interest Assessment should be conducted to ensure that the legitimate interests identified are not overridden by the interests or rights and freedoms of the Data Subjects. When the legal ground for a Processing activity is consent, the functions involved in the management of that Processing must verify that consent is freely given, specific, informed, unambiguous and duly documented.

The functions involved in the management of Processing activities must ensure that Data Subjects receive all necessary information under applicable data protection and privacy laws, including without limitation with regard to the purpose(s) of the Processing and the disclosure of their Personal Data to third parties.

Information provided to Data Subjects must be concise, intelligible and in clear and plain language. Information may be provided orally, in writing or by other means, including where appropriate, by electronic means.

Even where applicable law does not require the Data Controller to provide an information notice to the Data Subjects, Companies of the Bracco Group must implement appropriate measures to ensure that the Processing is carried out in a transparent manner (e.g. an information notice can be made available on the Controller Company's website and linked at the bottom of electronic communications).

5.2. PURPOSE LIMITATION

Personal Data may only be collected and processed for specific and legitimate purposes. Data Subjects must receive all appropriate information about the purposes of the Processing of their Personal Data from Data Controllers. Personal Data must not be processed in a manner that is incompatible with the purposes communicated to the Data Subject.

When Personal Data are transferred between Bracco Entities:

- the discloser shall communicate the initial purpose of the Processing to the recipient;

- the recipient shall take into consideration this initial purpose when further Processing and storing the Personal Data.

Changes of purpose are only allowed if appropriate information is provided to Data Subjects about the new purpose(s), and if their consent is collected or if another appropriate legal ground can apply, in accordance with applicable local laws and regulations.

5.3. DATA MINIMISATION

Companies of the Bracco Group must ensure they only collect or otherwise obtain Personal Data that is adequate, relevant and limited to what is necessary for the purpose of the Processing.

It is not permitted to hold Personal Data on a "just-in-case" basis, without clearly knowing the purpose of further Processing activities that may be carried out with this data.

5.4. DATA QUALITY AND INTEGRITY

Companies of the Bracco Group must ensure that the Personal Data they collect or otherwise obtain are factually correct and, as far as practicable, kept up to date. Appropriate measures should be promptly taken to correct or amend incorrect or incomplete data, in particular when a notification is received from a Data Subject regarding the inaccuracy of his or her data.

5.5. STORAGE LIMITATION

The periods of retention of Personal Data shall be limited to what is strictly necessary to fulfil the intended purpose of the Processing.

Anonymization of Personal Data should be used at an early stage, as far as practicable and appropriate in light of the intended purpose, in particular for Special Categories of Personal Data.

When it is not practicable or appropriate to anonymise Personal Data, the functions involved in the Processing of the data shall ensure that an appropriate retention period is defined and that appropriate procedures are implemented to delete the data upon termination of this period, in accordance with the relevant procedure.

5.6. LIMITATIONS ON THE PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

Special Categories of Personal Data involve data revealing, directly or indirectly, a Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data used for the purpose of uniquely identifying a natural person, data concerning a Data Subject's health, sex life or sexual orientation.

Special Categories of Personal Data and data relating to criminal convictions and offences are subject to specific rules because of their sen-

sitivity and/or confidentiality. In order to lawfully process Special Category and criminal offence Data, a lawful basis and a separate condition for the processing must be identified under applicable data protection laws and regulations.

5.7. REGISTRATION, AUTHORISATION AND NOTIFICATION

Each Company of the Bracco Group is responsible for complying with any registration, authorisation or notification obligation in the country(ies) where it operates. The functions involved in the management of Processing activities shall hence, before starting a project or initiative involving Personal Data and for the entire duration of the Processing, file the necessary registration statements, obtain the required authorisations and send notifications to the competent Data Protection Authority(ies) in accordance with applicable laws, regulations and recommendations.

5.8. TRANSFERS OF PERSONAL DATA

The transfer of Personal Data across national borders (including between Companies of the Bracco Group) is only permissible if those data are properly protected. A transfer of Personal Data within the European Union is generally permitted if the data have been lawfully collected and are processed in accordance with applicable local laws and regulations.

The transfer of Personal Data from an EU country to an non-EU country is permitted only if one of the following condition is met:

- The European Commission has established, in an adequacy decision, that the country of the recipient ensures an adequate level of protection of Personal Data;
- Standard Contractual Clauses or Binding Corporate Rules have been executed between the exporter and the importer;
- For transfers made on an occasional basis:
  - the Data Subject has explicitly consented to the transfer;
  - 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;
  - the transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, and the Data Subject is physically or legally incapable of giving consent; or
  - the transfer is made from a register which is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by applicable law for consultation of the register are fulfilled in the particular case.

Further transfer of Personal Data which have been transferred from an EU country to an non-EU country is permitted only if one of the above listed conditions is fulfilled. In any case, the Bracco Company who initially transferred the Personal Data outside of the EU shall receive appropriate information prior to any further transfer of Personal Data to another non-EU country. Similar rules shall be followed for transfers of Personal Data from Switzerland or the United Kingdom, subject to any changes to local laws, regulations and recommendations in those jurisdictions.

The transfer of Personal Data from other non-EU countries (e.g.: Mainland China) is permitted only if conducted in accordance with local national laws, regulations and recommendations.

5.9. SECURITY MEASURES

Companies of the Bracco Group shall define and implement appropriate control mechanisms and security measures for each Processing activity, in order to prevent data protection risks and mitigate the effects of Data Breaches.

In particular, each Company of the Bracco Group must, for each existing activity or before the implementation of any new activity involving the Processing of Personal Data, set up any appropriate technical and organisational security measures in order to avoid accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access of Personal Data.

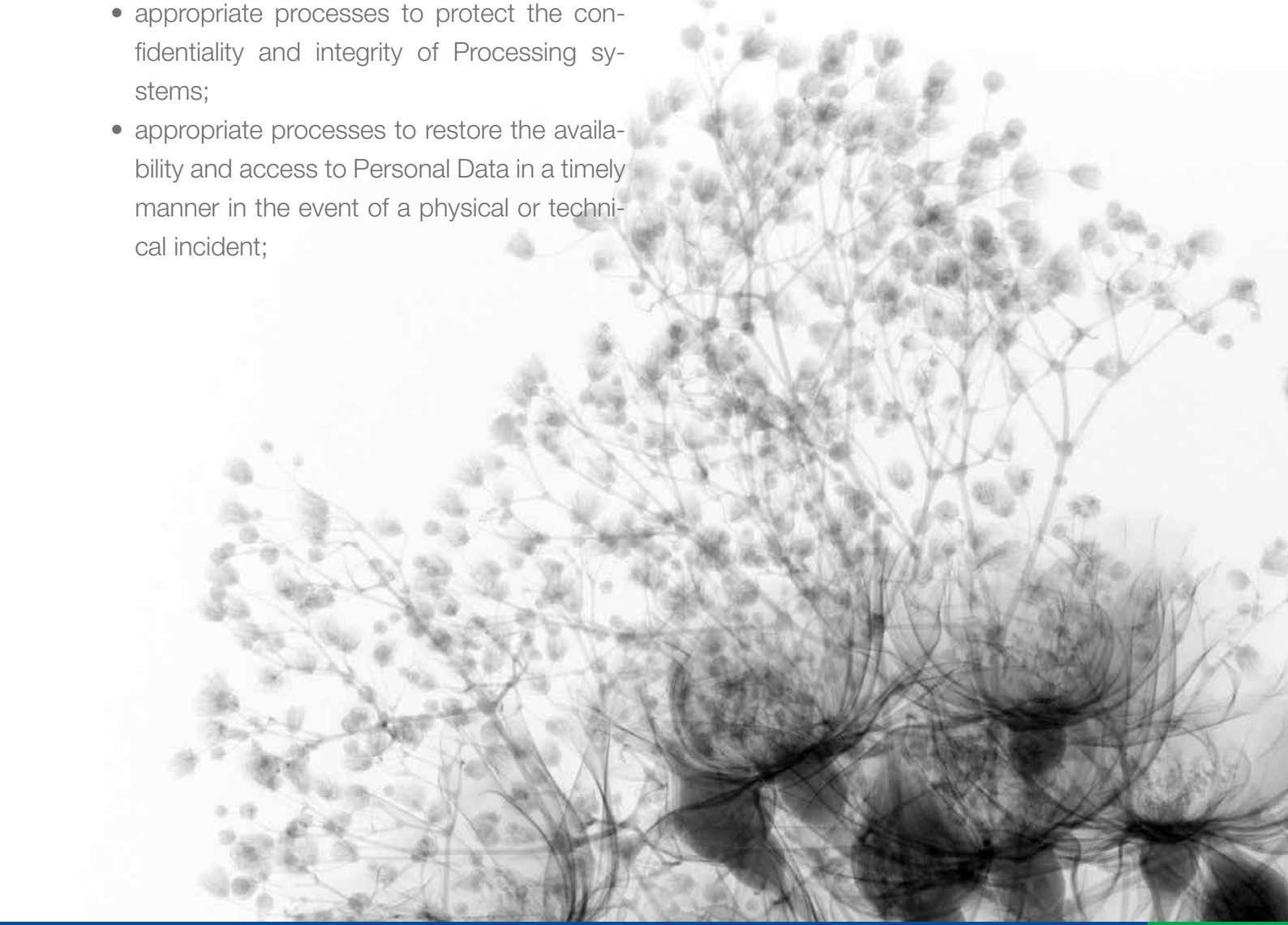
Security measures shall in particular involve:

- pseudonymisation, anonymisation or encryption of Personal Data;
- information security (e.g. controls of physical and logical access to Personal Data);
- appropriate processes to protect the confidentiality and integrity of Processing systems;
- appropriate processes to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
- appropriate processes to test, assess and evaluate the effectiveness of technical and organisational security measures on a regular basis.

5.10. TRAINING OF PERSONNEL

Companies of the Bracco Group must provide training to all their employees carrying out activities which involve the Processing of Personal Data.

During data protection training, the Personnel must receive all necessary information about the data protection standards to be followed within the Bracco Group, as well as the risks associated with any misconduct that could qualify as a breach of this Program, of the Data Protection Guideline and relevant Procedures or local SOPs and applicable laws and regulations.



6

ADDITIONAL PRINCIPLES

In addition to the general principles specified above, Companies of the Bracco Group must comply, as indicated in the Data Protection Guideline and applicable SOPs, with the following additional principles regarding:

(i) Data Breaches;
(ii) Privacy by Design and by Default;
(iii) Management of Data Subject Rights;
(iv) Management and update of the Records of Processing Activities;
(v) Data Retention;
(vi) Management of relationships with Data Processors.

6.1 GENERAL PRINCIPLES ON DATA BREACHES

Each Company of the Bracco Group shall put in place appropriate processes and procedures for the prevention, identification and remediation of any potential Data Breach, in accordance with the following principles.

It is the responsibility of any employee or contractor of a Company of the Bracco Group to report any actual, potential or suspected Data Breach to the competent functions.

It is the responsibility of all involved functions to follow this Program as they handle Data Breaches and implement the Data Protection Guideline and relevant Procedure and relevant local SOPs.

A. DATA BREACH REPORTING

Reporting of Data Breaches by employees

Companies of the Bracco Group must inform their employees and collaborators that they shall, when they become aware of an actual, potential or suspected Data Breach: (i) promptly report the incident to the Service Desk if it is related to IT systems (e.g. cyber-attack, loss of a laptop, etc.); or (ii) report the Breach to the competent security function if it is not related to IT systems (e.g. physical intrusion by unauthorized persons).

Reporting of Data Breaches by Data Processors

The functions responsible for negotiating and executing contracts with Data Processors must verify that those agreements impose on the Data Processors the obligation to promptly communicate to the Controller Company of any suspected or identified security incidents affecting the Personal Data transferred by the Company and/or processed on its behalf.

Reporting of Data Breaches by other subjects

Companies of the Bracco Group must inform Data Subjects and any other external stakeholders, either through their privacy notice or upon request, about the channels available to report an actual, potential or suspected Data Breach, and provide to the email addresses of the Group DPO or the competent Local DPO.

B. MANAGEMENT OF DATA BREACHES

All functions involved in the management of Data Breaches must ensure that incidents are addressed without delay and appropriately, in order to minimize the impact of the breaches and to prevent their recurrence.

Internal notifications

Companies of the Bracco Entity must immediately notify Personal Data Breaches that they identify or become aware of to the Group DPO, to the Local DPO or Privacy Focal Point and to the ITS Department.

Risk assessment

The functions involved in the management of Personal Data Breaches must promptly carry out a risk assessment, which must include at least the following elements:

(i) a description of the breach and its circumstances (i.e. Loss of Confidentiality, Loss of Integrity, Loss of Availability, Malicious Intent);
(ii) a definition of the categories of Personal Data affected by the breach (Basic Personal Details, Professional Life/Financial Data, Special Categories of Personal Data or Data relating to Criminal Convictions and Offences, etc.);
(iii) an estimation of the number of Data Subjects involved in the Breach;
(iv) an evaluation of the ease of identification of Data Subjects;
(v) a verification of whether the data affected by the Breach is intelligible or not (i.e. whether it is protected by encryption or pseudonymisation or not); and
(vi) an evaluation of the related risk levels, based on all the above elements.

Notification to the competent Data Protection Authority(ies)

Data Breaches must be notified by the competent Data Protection Authority(ies) and, as the case may be, to other supervisory authorities in accordance with applicable laws and regulations.

The notification must be made without delay, and in any case within the time limit specified in local laws and regulations.

The notification shall at least indicate:

(i) the nature of the Personal Data Breach, the categories and approximate number of Data Subjects concerned and the categories of Personal Data affected by the Breach;
(ii) the name and contact details of the Group DPO, Local DPO or Privacy Focal Point, as appropriate;
(iii) the likely consequences of the Personal Data Breach; and
(iv) the measures taken or proposed to be taken by the controller to address the breach and to mitigate its possible adverse effects.

Communication to Data Subjects

Companies of the Bracco Group shall notify Personal Data Breaches to Data Subjects when such communication is required under applicable laws and regulations or requested by the competent Data Protection Authority.

Communication to Data Subjects is in particular required when the Data Breach is likely to cause a high risk for the Data Subjects. Subject to any contrary legal or regulatory provi-

sion, communication to Data Subjects shall not be required if any of the following conditions is met:

(i) the affected Company had, before the breach, implemented appropriate technical and organisational protection measures (e.g. measures that make Personal Data unintelligible to any person who is not authorised to access it, such as encryption);

(ii) the affected Company has taken subsequent measures which ensure that the risks for Data Subjects are no longer likely to materialise (e.g. has identified the person who misappropriated the data and prevented them from using it in any manner);

(iii) communication to Data Subjects would involve disproportionate effort. In such a case, there shall be instead a public communication or similar measure whereby the Data Subjects are informed in an effective manner (e.g. communication through a banner on the affected Company's website).

The communication provided to Data Subjects shall be given in clear and comprehensible language, and include at least the following information:

(i) the name and contact details of the Group DPO, Local DPO or Privacy Focal Point, as appropriate;

(ii) the likely consequences of the Personal Data Breach; and

(iii) the measures taken or proposed to be taken by the controller to address the breach and to mitigate its possible adverse effects.

6.2 GENERAL PRINCIPLES ON PRIVACY BY DESIGN AND BY DEFAULT

Companies of the Bracco Group shall follow a Privacy by Design and by Default approach, i.e. take into account privacy measures before starting a new project or initiative. They must, when required by this Global Program or applicable laws and regulations, carry out Data Protection Impact Assessments (or any similar analysis required by local law) in order to identify the appropriate safeguards to implement to protect the rights of Data Subjects.

It is the responsibility of all involved functions to follow this Program and the Global Data Protection Guideline as they consider implementing new projects or modifying existing Processing activities, implement the related Global Procedure and the relevant local SOPs.

A. PRIVACY BY DESIGN AND DEFAULT

Each Company of the Bracco Group shall, by design before the implementation of any new activity involving the Processing of Personal Data and by default for each existing activity, implement any appropriate measure to comply with applicable data protection laws and regulations in an effective manner and protect Personal Data.

The functions involved in the management of Processing activities must ensure that only the Personal Data which is necessary for the purpose of the Processing activity is collected and processed. They must also verify that appropriate safeguards, including security measures, are put in place to protect Personal Data and prevent Data Breaches.

B. ANALYSIS OF THE RISKS FOR DATA SUBJECTS AND DATA PROTECTION IMPACT ASSESSMENTS

Assessment of the risks associated with new or updated projects and activities

Before starting a new project involving the Pro-

cessing of Personal Data or updating a Processing activity (e.g. using new methods for an existing project), the involved functions shall determine the risks associated with the new or updated initiative. Such assessment can be carried out with the help of the Privacy Tool.

New Processing activities which are likely to create a high risk for Data Subjects cannot be started before further analysis has been carried out, including a Data Protection Impact Assessment when required by applicable laws or regulations, in order to identify the necessary measures to protect the rights of Data Subjects.

Evaluation of whether a Data Protection Impact Assessment is necessary

Data Protection Impact Assessments ("DPIA") (or any equivalent analysis required by applicable laws and regulations) must be performed before implementing Processing activities which, because of their nature, scope, context or purposes, are likely to create a high risk for the rights and freedoms of Data Subjects.

The following criteria should in particular be considered when determining whether to undertake a DPIA:

(i) The Processing involves evaluation or scoring (which include profiling and predictive activities);

(ii) The Processing involves automated decision making with legal or similar significant effect (e.g. the Processing may lead to the exclusion or discrimination against individuals);

(iii) The Processing involves systematic monitoring (i.e. is used to observe, monitor and control Data Subjects);

(iv) The Processing involves Special Categories of Personal Data or Personal Data of a highly personal nature;

(v) The Processing involves Personal Data concerning vulnerable Data Subjects (e.g. children);

(vi) The Processing involves the combination or matching of several datasets;

(vii) Personal Data is processed on a large scale – in order to define whether the Processing is carried out on a large scale, the following factors should be considered: the number of Data subjects concerned; the volume of data and/or the range of different data items being processed; the duration or permanence of the data processing activity; and the geographical extent of the Processing activity;

(viii) The Processing involves an innovative use or application of technological or organizational solutions (e.g. combination of finger print and face recognition for physical access control);

(ix) The Processing in itself prevents Data Subjects from exercising a right or using a service or a contract.

Performance of the DPIA

The aim of a DPIA is to identify the risk level associated with a Processing activity and to evaluate the necessity and proportionality of the Processing.

A DPIA shall involve at least the following steps:

(i) An analysis of the context of the Processing, which shall include the identification of the nature, scope, context and purposes of the Processing and of the sources of the risks;

(ii) An assessment of the likelihood and severity of the inherent risks of the Processing for Data Subjects;

(iii) The measures considered to mitigate the risks and to ensure that Personal Data are protected and that applicable laws and regulations are complied with.

A DPIA may cover a single Processing activity or a set of Processing operations that are similar in terms of nature, scope, context, purpose, and risks.

Each DPIA shall be reviewed regularly, in particular when a change is made to the initiative for which the assessment was performed.
Processing activities which are likely to create a high risk can be implemented only if the DPIA demonstrates that the inherent risks are in fact not likely to happen or to have severe consequences.

Consultation of the supervisory authorities

The involved functions shall consult the competent Data Protection Authority(ies) prior to the implementation of the Processing if the DPIA indicates that this Processing would result in a high risk in the absence of mitigation measures and in any case when foreseen by applicable laws and regulations.
Each Company of the Bracco Group must follow any advice provided by the Data Protection Authority and comply with any of its decisions.

6.3 GENERAL PRINCIPLES ON MANAGEMENT OF DATA SUBJECT RIGHTS

Companies of the Bracco Group must enable Data Subjects to exercise the rights granted to them by applicable data protection laws and regulations. They must implement appropriate processes to ensure that Data Subjects' requests are handled in an efficient and timely manner.
It is the responsibility of all involved functions to follow this Program and the Data Protection Global Guideline as they manage inquiries and requests from Data Subjects, implement the related Global Procedure Guidelines and relevant local SOPs.

A. COMMON PRINCIPLES

Collection of the requests

Data Subjects must be informed about the official channels that they can use to exercise their rights (i.e. they can send an email to the Group DPO and, when applicable, to the Local DPO, send a letter to the relevant Company or fill an online form on a Company's website).
Some requests can be received through unofficial channels (e.g. during a phone or face-to-face conversation between a Data Subject and an employee of a Company of the Bracco Group, through the contact section of a Company's website, through an email sent to an employee's email address). Such requests shall be immediately forwarded to the Group DPO and, when applicable, to the Local DPO.

Processing of the requests

The functions involved in the management of requests relating to Data Subject rights shall, before processing a request, confirm the identity of the applicant (and of the Data Subject, when he or she is not the applicant) and verify that Personal Data concerning the Data Subject is indeed collected or stored by the Bracco Group. They must then evaluate whether the request is valid under applicable laws and regulations and whether it is feasible to comply with the request, in cooperation with the ITS Department.
The involved functions can provide a negative response to a Data Subject's request relating to the exercise of his or her rights only: (i) if they do not receive sufficient information from the applicant to fulfil the request; or (ii) if applicable laws or regulations allow them to refuse to comply with the request.
Data Subjects' requests and inquiries shall always be treated in a confidential manner (Bracco Group's and Companies' staff shall be involved on need to know basis).

Timely response

The functions involved in the management of requests relating to Data Subject rights must respond to each request without undue delay, and at the latest within one month of the receipt of that request (unless a different time limit is specified by applicable laws and regulations). That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The involved functions shall inform the Data Subjects of any such extension within one month of the receipt of the request, and explain to them the reasons for the delay.

B. TYPES OF DATA SUBJECT RIGHTS' REQUESTS

Requests relating to the right of access

Companies of the Bracco Group shall, upon receipt of right of access requests, send to the Data Subjects a confirmation as to whether or not their Personal Data are being processed and, where this is the case, provide them with a copy of the Personal Data and with all appropriate and relevant information under applicable laws.

The functions involved in the management of right of access requests shall identify the most appropriate means of complying with the requests, on the basis of the following criteria: (i) categories of Personal Data involved; (ii) format of the Personal Data; (iii) channel used by Data Subjects to exercise their rights; and (iv) volume of Personal Data to be transferred to the Data Subject.

They must ensure that the copies of Personal Data sent to Data Subjects do not include information relating to other Data Subjects or information that is exempt from the right of access under applicable laws and regulations and that the fulfilment of right of access requests does not adversely affect the rights of other Data Subjects.

Requests relating to the rights of rectification and erasure

Companies of the Bracco Group shall, upon receipt of requests relating to the right of rectification, complete or rectify incomplete or inaccurate Personal Data.

They shall also, upon receipt of requests relating to the right of erasure, erase Personal Data relating to the Data Subject if:

(i) The Personal Data is no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(ii) The Data Subject has withdrawn his or her consent and there is no other legal ground for the Processing;
(iii) The Data Subject has objected to the Processing and there is no other legal ground for the Processing;
(iv) Personal Data has been unlawfully processed;
(v) Personal Data has to be erased for compliance with applicable laws and regulations.

The involved functions must assess on a case-by-case basis if the exercise of the right of erasure can be limited in accordance with applicable laws and regulations.

When Personal Data has been transferred to another Data Controller or to a Data Processor, the involved functions must take reasonable steps to inform the recipients that the Data Subject has exercised his or her right of rectification or erasure.

Requests relating to the right to data portability

Companies of the Bracco Group shall, upon receipt of portability requests, send to the Data

Subjects their Personal Data in a structured and machine-readable format and/or, if technically feasible, transfer their Personal Data to another Data Controller designated by the Data Subject.

The functions involved in the management of portability requests shall identify the most appropriate alternative to comply with the request, on the basis of the following criteria: (i) categories of Personal Data; (ii) format of the Personal Data; (iii) channel used by Data Subjects to exercise their rights; and (iv) volume of Personal Data to be transferred to the Data Subject or other Controller. They must ensure that the Personal Data sent to the Data Subjects or to other Controllers do not include information relating to other Data Subjects and that the fulfilment of portability requests does not adversely affect the rights of other Data Subjects.

Requests relating to the right to request restriction of processing

Companies of the Bracco Group shall, upon receipt of a request relating to the right to restriction and after having verified that the conditions set out by applicable laws and regulations are fulfilled, restrict the Processing of the Data Subject's Personal Data.

The functions involved in the management of right to restriction requests shall identify the most appropriate alternative to comply with the request (e.g. transferring the data into a different information system in which the Data will not be processed, applying stricter access control measures, etc.).

Requests relating to the right to object to a Processing

Companies of the Bracco Group shall, upon receipt of a request relating to the right to object and after having verified that the Processing is based on public interest or legitimate interests and that the Data Subject's particular situation justifies a restriction, stop the Processing of the Data Subject's Personal Data.

They must also stop the Processing of a Data Subject's Personal Data for marketing purposes promptly upon receiving an objection notice, without asking the Data Subject for justification.

C. ADMINISTRATIVE MANAGEMENT OF THE REQUESTS

Management fees

No cost or fee shall be charged to Data Subjects for the management of the inquiries or requests relating to the exercise of Data Subject rights. However, if the requests from a Data Subject are unfounded or excessive (e.g. the Data Subject sends repetitive requests to the same Controller Company), the functions involved in the management of the requests may charge a reasonable fee, based on the administrative costs incurred to provide information or to take the required action.

Record keeping

Each Company of the Bracco Group must keep records of all documentation relating to the requests received from Data Subjects and related internal verifications and audits.

6.4 GENERAL PRINCIPLES ON MANAGEMENT AND UPDATE OF THE RECORDS OF PROCESSING ACTIVITIES

It is the responsibility of all involved functions to follow this Program and the Global Data Protection Guideline as they create, maintain, update or review Records of Processing Activities, implementing the related Global Procedure and the relevant local SOPs.

A. CONTENT OF THE RECORDS OF PROCESSING ACTIVITIES

Each Company of the Bracco Group shall maintain a Record of Processing Activities, which must contain at least the following information (the Privacy Tool can be customized at global and local level specifying additional information):

(i) Contact details of the Company;
(ii) Contact details of the functions involved in the Processing activities, of the Group DPO and of the Local DPO/Privacy Focal Point;
(iii) For each Processing activity:
  (i) the purposes of the Processing;
  (ii) the categories of Personal Data and Data Subjects involved;
  (iii) the recipients or categories of recipients to whom the Personal Data is disclosed or will be disclosed;
  (iv) if applicable, transfers of Personal Data to third countries;
  (v) the retention periods for each category of Personal Data;
  (vi) the technical and organisational security measures implemented to protect the Personal Data collected, used or retained in relation to the Processing.

B. UPDATE OF THE RECORDS

Companies of the Bracco Group shall ensure that the information contained in the Records is kept up-to-date at all times.

Update of the Records in relation to new or modified Processing activities

Companies of the Bracco Group shall update the Records as appropriate whenever a new activity or a change to an existing activity involving the Processing of Personal Data is implemented. The Records shall in particular be updated if one the following events occurs:

(i) New business projects or initiatives;
(ii) Changes in the Company organisation chart;
(iii) Changes in the information system;
(iv) Collection of new categories of Personal Data;
(v) Appointment of new suppliers;
(vi) New transfers of Personal Data;
(vii) Any other event that may impact the characteristics of the processing

Annual review of the Records

In addition to the updates mentioned above, the functions responsible for maintaining the Records of Processing Activities must review those Records at least annually. They shall, during each review, update the Records to take into account any change made to existing Processing activities and any new activity involving the Processing Personal Data which has not been previously included in the Records.

6.5 GENERAL PRINCIPLES ON GLOBAL DATA RETENTION

It is the responsibility of the involved functions to follow this Program and the Data Protection Guideline as they manage the storage, deletion or anonymisation of data and records, implement the related Global Procedure and the relevant local SOPs.

Definition of appropriate retention periods

Companies of the Bracco Group shall ensure that each category of record or data, including Personal Data, is retained only for the necessary duration in accordance with applicable laws and regulations.

In particular, Personal Data must not be kept in

a form which permits identification of Data Subjects for longer than is necessary for the purposes for which these Data are processed.
Companies of the Bracco Group shall in particular comply with the retention periods specified in the Data Retention Schedule included in the relevant Data Protection Guideline, unless shorter retention periods are imposed by applicable laws and regulations or unless it is necessary for them to retain data for a longer period of time (in particular to comply with their legal obligations or to maintain evidence for the establishment, exercise or defence of legal claims).

Deletion and anonymisation of data and records

The functions involved in the management of data and records shall verify that all data and records are destroyed, deleted or anonymised in a secure manner upon expiration of the defined retention period. Data and records may also be pseudonymised, upon expiration the defined retention period, to ensure that financial activities and statistics can be conducted; in such a case, a procedure must be implemented to restrict access to Personal Data only to system administrators in specifically defined circumstances.
The means employed for destroying or deleting the data and records shall prevent any subsequent unauthorised access to the information (e.g. paper records shall be shredded, etc.).
All copies of the same data or records shall be destroyed, deleted or anonymised simultaneously, regardless of their format.

Data and records retained by third parties

Where a Company of a Bracco Group appoints a third party to maintain records or data on its behalf or to manage its IT systems, it must ensure that the contract executed with this third party expressly provides for the deletion of all records and data and copies thereof upon request of the Company or at the latest upon termination of the contract.

6.6 GENERAL PRINCIPLES ON MANAGEMENT OF RELATIONSHIPS WITH DATA PROCESSORS

It is the responsibility of all involved functions to follow this Program and the Data Protection Guideline as they appoint and execute agreements with Data Processors, implement the related Procedure and the relevant local SOPs.

Selection of Data Processors

Companies of the Bracco Group shall only select and use Data Processors who provide sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a manner that the Processing will meet the requirements of this Data Protection Program and of applicable laws and regulations.
Before appointing a Data Processor, Companies of the Bracco Group must in particular verify that the Processor will implement appropriate security measures to the Personal Data that it will process on their behalf, in light of the state of the art and the nature, scope, context and purposes of the Processing.

Contracts with Data Processors

The functions involved in the appointment and management of Data Processors must ensure that each and every contract signed with a Data Processor clearly and precisely identifies the Processing activities that will be carried out by the Processor, the purpose(s) of the Processing and the Personal Data that will be transferred to this Processor. They must also verify that the contract contains all the mandatory provisions in accordance with applicable laws

and regulations (e.g. article 28 of the GDPR for Processing activities in GDPR scope).

Companies of the Bracco Group must also ensure that, when they process Personal Data on behalf of a third party who acts as a Data Controller, their contract with the Data Controller appropriately describes the Processing activities that they must carry out as Data Processor and contains the provisions required by applicable laws and regulations. Companies of the Bracco Group acting as Data Processors shall in any case comply with the Data Protection Program.

Appointment of Sub-Processors

All contracts entered into between a Company of the Bracco Group and a Data Processor must specify that the Processor can only appoint a Sub-Processor after having obtained the authorisation of the Bracco Company to do so (or, as appropriate, after having provided appropriate information to Bracco).

Companies of the Bracco Group must request their Data Processors to represent and warrant that they will contractually impose on their Sub-Processors data protection obligations substantially identical to the ones as set out in their contract with the Controller Company and that, if the Sub-Processor fails to comply with its obligations relating to protection of Personal Data, the Data Processor will remain fully liable to the Controller Company for the non-performance by the Sub-Processor of its obligations. Data Processors shall also represent and warrant that they will require their Sub-Processor located outside the EU to execute Standard Contractual Standards.

Audit to Data Processors

Processors should be regularly audited under the responsibility of the Bracco functions involved in the execution of contracts and the management of relationships with such Processors, availing itself of the local/group DPO and of ITS assistance as the case may be.

Record keeping

The functions involved in the execution of contracts and the management of relationships with such Processors shall retain a copy of the Data Processing Agreements executed with the Processors and of any correspondence exchanged between the Controller Company and the Processor.

7

OTHER RELEVANT **DOCUMENTS**

- Glossary
- Guideline on “Data Protection”
- Bracco Group Code of Ethics.

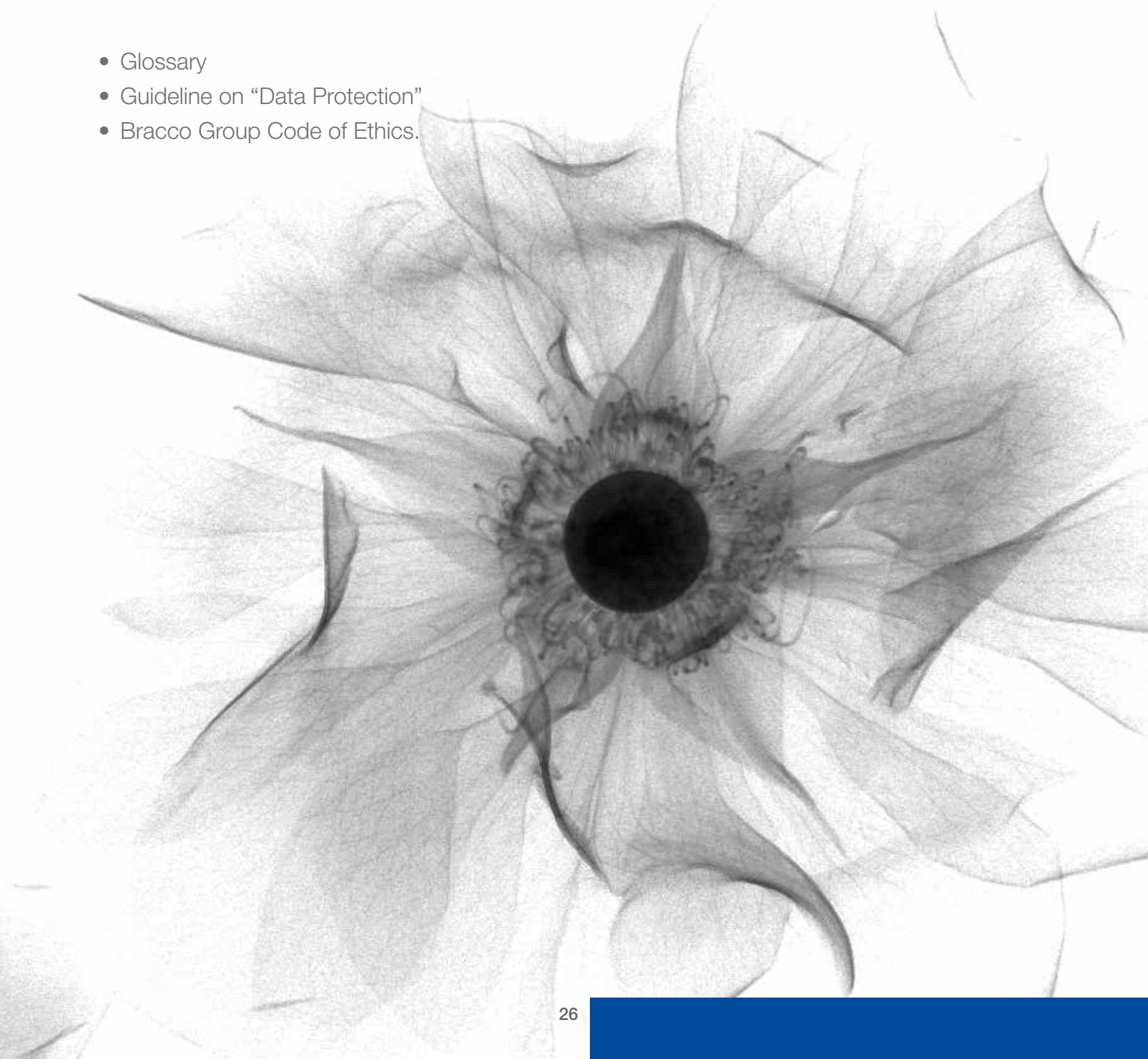


Table of Contents

LIFE FROM INSIDE

data protection program

Edited by:
Edited by Global Legal, Compliance and Corporate Affairs
Bracco Group Image&Communication

www.bracco.com