Bracco Imaging Group
Data Protection Program

LETTER FROM THE CEO

Data protection is an increasingly important issue in the life science industry. All individuals expect protection of their personal data.

Bracco Imaging Group respects individual privacy and is committed to protect the personal data of its customers, employees, clinical trial participants, business partners and other data subjects, in accordance with the data protection laws in force in all the Countries where Bracco Imaging Group operates. We believe that any person who works in our Group shall adhere to the highest international 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. This includes the right of the individuals to be informed of and make decisions as far as the processing of their personal data is concerned.

The Bracco Imaging Group's Data Protection Program was launched to assure the compliance with rules. The Program is meant to ensure that everything we do is in conformity with the existing policies and procedures as well as all the applicable laws and regulations.

The Bracco Imaging Group's Data Protection Program sets out the requirements for ensuring that we collect, use, retain and disclose personal data in a fair, transparent and secure way.

The Chief Executive Officer

Fulvio Renoldi Bracco

Sommario

INTRODUCTION

The Group Data Protection Program (hereinafter referred to as the "Program") applies to Bracco Imaging Group and Acist Medical Systems Group (hereinafter collectively referred to as "Group") and their Business Partners, including consultants working on their behalf. The Program is inspired and was elaborated to complement the Code of Ethics and provides the standards to guarantee that Group activities are conducted with the highest values of ethics and integrity and in compliance with local and international data protection laws, regulations and practices.

The implementation of the Program in every country where the Group operates is mandatory. Each company shall organize and implement control activities over the existing processes to prevent data protection risks. The following are the **key responsibilities** regarding the Program.

It is responsibility of any **Bracco Personnel** to ensure that the Program is fully implemented and its principles and data protection processes are constantly followed.

It is responsibility of the **Group Data Protection Officer** (hereinafter referred to as Group "DPO") to coordinate the implementation of the Program across the Group, with the support of the Group Privacy Committee, Local Data Protection Officers and local Privacy Focal Points, as specified in Annex A, by assigning clear objectives to each company and monitoring and evaluating their performances in the implementation phase. In particular, Group DPO key responsibilities are:

- monitoring the adoption and the update of the Program;
- providing advice about the data protection topics;
- facilitating Program training within the Group;
- monitoring constantly the implementation of the Program with the support of the Corporate Internal Audit and professional advisors;
- carrying out investigations where potential Program breaches were identified.

In order to ensure a proper implementation of the Program both **internal and external communications** are of huge importance , in particular:

- **internal communication** aims at informing Personnel about the importance of Personal Data protection;
- **external communication** aims at raising awareness among third parties about the Group commitment towards Personal Data protection.

For communication purposes, the Program is available for consultation to Personnel through the Group Intranet and to external stakeholders through the Group internet webpage.

To ensure that the Personnel is aware of the data protection standards in place, as well as being aware of the risks related to any misconduct that could breach the rules defined within the Program or the applicable laws and regulations, data protection training is provided.

Allegations of data protection violations might be sent to the Group DPO (dpo@bracco.com) and/or through the whistleblowing channel (corporateIA@bracco.com). Anyone submitting a notice will be protected from any harassment, retaliation, victimization or discriminatory behaviour. The identity of the person submitting a notice will be kept confidential.

The Group shall take adequate **disciplinary measures** (*e.g.* warning, suspension, dismissal and/or even legal action) and reserves any additional remedy, according to the provisions of any applicable laws and regulations, if any Group Personnel intentionally or negligently breaches any of the provisions of this Program.

Scope and applicability

The data protection and data security principles contained within this Program are binding on all Bracco Entities. Each Bracco Entity shall integrate the principles through procedures, guidelines and notices that are consistent with this Program.

Existing legal obligations - both national and international - shall prevail over this Program in countries where the processing of personal data occurs. Every Controller/Processor of Personal Data must therefore check whether those obligations apply in his/her field of responsibility and ensure the relevant compliance.

However, where data protection requirements under national or international law applicable to Personal Data processing are less strict than the present Program, the principles of this Program shall prevail.

Each Bracco Entity is responsible for complying with any notification and registration obligations in its respective country/es. The transfer of Personal Data to national authorities and agencies is allowed only in accordance with the respective applicable national laws.

Whenever a Bracco Entity has reason to believe that legal obligations are preventing it from fulfilling its obligations under this Program, it shall immediately notify the Group DPO, unless prohibited by a law enforcement agency under national law.

The Bracco Entity shall then make a responsible decision on the matter in agreement with Group DPO and, if necessary, shall notify the respective national Supervisory Authority accordingly.

Data subjects' categories involved

This Program applies to the Processing of Personal Data of any individual whose Personal Data are processed by and on the behalf of a Bracco Entity (acting as Controller or Processor). Existing data processing activities carried out across Bracco Entities are mainly related to the following data subjects' categories:

- employees;
- healthcare professionals (i.e. HCPs);
- patients enrolled in clinical trials;
- patients/subject to post marketing surveillance;
- customers;
- suppliers;
- other business partners.

1. General principles for processing personal data

Bracco Entities shall observe the following **data protection principles** when collecting, processing and storing individuals' Personal Data. Each Bracco Entity is responsible for complying with the same principles and must be able to demonstrate the organization's compliance practices.

1.1. Lawful, Fair and Transparent personal data processing

Personal data shall be processed lawfully, fairly and in a transparent manner.

The Data Subject as well as any entity from whom or which Personal Data are collected, shall be informed, in accordance with the applicable law, about the purpose of the Processing of Personal Data and the possible transfer of Personal Data to Third Parties. In any case, where the information notice to Data Subject is not mandatory according to the local applicable law (e.g.: U.S. based HCP), Bracco Entities will implement the appropriate means to comply with the transparency principles set forth in this paragraph (e.g.: an HCPs information notice available on the company website that could be linked in electronic communications, etc.).

This Data Protection Program requires that the information must comply with the following rules:

- it must be concise, transparent, intelligible and simple;
- clear and plain language must be used;
- it must be provided orally, in writing or by other means, including where appropriate, by electronic means;

1.2. Intended purpose

Personal Data may only be collected and processed for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes.

When Personal Data are transferred between Bracco Entities:

- the discloser shall communicate to the Recipient the intended purpose of the Processing, and
- the Recipient shall take in consideration the intended purpose of the Processing of Personal Data transferred when further Processing and storing this data.

Changes of purpose are only allowed with the consent of the Data Subject or if permitted by national law in the respective country from which Personal Data are transferred.

1.3. Data retention

The time range for the processing of Personal Data should be strictly necessary to fulfil the intended purposes. Anonymization of Personal Data, if feasible, should be used at an early stage, as far as this is possible and the cost is appropriate to the intended protective purpose. This applies in particular with regard to the Processing of Special Categories of Personal Data.

Additional details regarding data retention approach are defined within the Annex F.

1.4. Data quality and integrity, data minimization

Personal Data must be factually correct and, as far as necessary, kept up-to date. Appropriate and reasonable measures should be taken in the shortest possible time to correct or amend incorrect or incomplete data.

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

1.5. Special Categories of Personal Data

Special Category of Personal Data shall mean data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and 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.

1.6. Data Processing Record

Each Bracco Entity shall maintain a Record of Processing Activities that contains the following information:

- Bracco Entity contact details;
- name and contact details for each role, such as Processor, the Group DPO and the Privacy Focal Point/Local DPO;
- purposes of the Processing;
- indication of the Data Subjects and Personal Data categories;
- categories of Recipients to whom the Personal Data have been or will be disclosed;
- where possible, the data storage periods for erasure of the different data categories;
- general description of the technical and organizational security measures implemented.

Additional details regarding updating and review of the Record of Processing Activities are defined within the Annex E.

1.7. Privacy by Design and by Default - Data Security

Bracco Entity shall by design implement any appropriate technical and organisational security measures to avoid accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access of Personal Data.

Furthermore, each Bracco Entity shall implement measures to ensure that only Personal Data which are necessary for each specific purpose of the processing are processed (by default).

These measures refer in particular to ICT systems (i.e. server, clients, workstations, networks and communication links, operating systems, DB, and applications). The security measures implemented to avoid unauthorized Personal Data processing include:

- information security (physical and logical access);
- input of data into data processing systems;
- data processing within processing systems;
- output of data from data processing systems;
- data transfer among different processing systems.

In addition, appropriate measures should be adopted to protect data against unauthorized access, modification, deletion or loss. They can include:

- pseudonymization, minimization and encryption of Personal Data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
- a process for testing, assessing and evaluating the effectiveness of technical and organisational measures on a regular basis to ensure the security of the Processing.

Additional details regarding Privacy by Design model are defined within the Annex C.

Additional details regarding Data Security approach are defined within the security measures in the use of corporate IT tools, as well as in case they are amended and supplemented.

1.8. Data Protection Impact Assessment

This Data Protection Program requires greater responsibility from the Controller and Processor towards the protection of Personal Data. In order to do that, it is necessary to introduce a privacy risk-based approach for

the identification of the appropriate measures to protect Personal Data and the relevant activity to evaluate the impact on the Personal Data protection through a Data Protection Impact Assessment (hereafter "DPIA").

The DPIA aims to identify the risk level exposure associated to Processing of Personal Data, as well as an evaluation of the need and proportionality of the Processing.

A DPIA may relate to a single Processing or more than an analogous operation in terms of nature, scope, context, ends and risks.

When the processing activity is likely to result in a high risk to the rights and freedoms of natural persons, DPIA should be conducted prior to processing Personal Data by every local department/function. However, a continuous review of the DPIA should be provided, repeating the evaluation on a regular basis.

Additional details regarding Data Protection Impact Assessment process and methodology are defined within the Annex C.

1.9. Data Breach

Each Bracco Entity shall put in place processes and procedures for the prevention and remediation of any possible data breach.

After the detection of a Personal Data Breach, the Bracco Entity shall notify the Data Breach to the Group DPO, Local DPO, Privacy Focal Point – as the case may be - and the Chief Information Security Officer.

Additional details regarding Data Breach process and document templates are defined within the Annex B.

2. Data Subjects Rights

Data Subjects may contact Bracco Entities (global or local functions) at any time with any inquiries and complaints regarding Processing activities of Personal Data. Such questions and complaints will be tracked and treated confidentially.

Details regarding Data Subjects Rights management are defined within the Annex D.

3. Contract Data Processing

Where Processing activities are carried out on behalf of a Bracco Entity acting as Controller, the Controller before starting the Processing shall choose a Processor providing sufficient guarantees to implement appropriate technical and organizational measures and procedures in such a way that the Processing will meet the requirements of this Data Protection Program and any applicable law.

Additional details regarding Contract Data Processing management are defined within the Annex G.

4. Export of Personal Data

4.1. General premises

The transfer of Personal Data across national borders is only permissible if data are properly protected.

A transfer of Personal Data within the European Union (EU) is generally permitted if processing of the data is also permitted according to section 1.1.

4.2. Export of Personal Data from EU outside the EU

Based on this Data Protection Program, the transfer of Personal Data from an EU country to an extra-EU country is permitted only if one of the following condition is met:

- the Data Subject has explicitly consented to the proposed transfer; or
- 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; or

- 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; or
- the transfer is necessary for important reasons of public interest; or
- the transfer is necessary for the establishment, exercise or defence of legal claims; 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; or
- the transfer is made from a register which according to the law 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 the law for consultation are fulfilled in the particular case;
- the extra-EU country, a territory or one or more specified sectors within that extra-EU country, or the international organisation in question ensures an adequate level of protection; or
- Standard Contractual Clauses or Binding Corporate Rules.

4.3. Export of Personal Data between non-EU countries

Further transfer of Personal Data, which have been transferred from the EU to an extra-EU recipient, is only permitted, subject to section 1.1, if extra-EU recipient country has an adequate data protection standard or if one of the circumstances described in section 4.2 of this Data Protection Program applies. In any case, the Bracco Entity in the EU that transferred the Personal Data shall be informed prior further transfers of Personal Data to another extra-EU country.

The transfer of Personal Data from an extra-EU county to another extra-EU county as a general rule is only permitted in accordance with local national laws.

5. Annexes

- Annex A - Privacy Governance Guideline
- Annex B - Data Breach Process Guideline
- Annex C - Privacy by Design & by Default Model - Focus on DPIA Methodology - Guideline
- Annex D - Data Subject's Rights Management Guideline
- Annex E - Updating Processes of the Record of Processing Activities Guideline
- Annex F - Data Retention Guideline
- Annex G - Third Party Management Guideline
- Annex H - Glossary