doValue

"Privacy and security of data and information"

CONTENTS

1 SECTION: "PRIVACY AND SECURITY OF DATA AND INFORMATION"

In a continuously evolving and increasingly interconnected global context, new vulnerabilities and threats increase the risks related to the processing of Personal Data and information security in all phases of their life cycle, from collection to disposal.
Within the company context, all personnel employed by doValue Group companies find themselves acquiring a large amount of personal data and confidential information of customers, suppliers and other stakeholders, entailing various regulatory and business requirements.
The protection of data and information is, therefore, a priority of the doValue governance and business model, as this crucially influences the protection of the brand, the reduction of operating losses, the quality of customer relations, the level of confidence with all stakeholders and compliance with of regulatory obligations.
doValue has therefore started up a **personal data and confidential information protection programme** consisting in the adoption of the following Programmes:

- Personal data protection
- Confidential information protection;
- Technical measures and procedures (Cyber Security) on both personal data and on confidential information

1.1 PERSONAL DATA PROTECTION PROGRAMME

The General Data Protection Regulation, officially Regulation no. 2016/679 and known by the acronym "GDPR", which entered into force in May 2016 and became effective from 25 May 2018, made significant changes to the data protection legislation.
The Regulation, which applies to all data processing and the protection of information carried out by European Union Member States, guarantees individuals greater rights of control over their personal data and attributes to organisations the responsibility for adopting adequate measures to protect personal data.
The doValue Group has identified and adopted appropriate technical and organisational measures with a view to strengthening the protection of the processed personal data, in respect of the principle of *accountability*, and to guarantee the security and protection of the personal data processed by its personnel through a risk-based approach, in line with the applicable regulatory requirements and with the expectations of the data subjects.

1.1.1 Types of personal data processed

The Group's core business is the management of non-performing loans on behalf of Third Parties (e.g. Principals/Banks/SPV), in other words all ancillary judicial and extrajudicial activities directly or indirectly connected with the core activities described above.

In this context, the doValue Group Companies find themselves managing:

- different types of Personal Data (i.e. Identification, Sensitive / Special, etc.);
- different categories of data subjects in relation to which they act as both Controllers (employees, customers, potential customers, third parties, etc.) and External

Processors (i.e. data owned by the principal Banks referring to obligated parties, processed as part of credit recovery mandates).

1.1.2 How the doValue Group demonstrate compliance with the GDPR?

A robust personal data protection system is a fundamental requirement in organisations operating in the financial sector. The growing demand for reliability and conformity with specific requirements involves, on the one hand, an increase in the complexity level for the management of cyber risks and, on the other, an increase in the level of confidence of customers in the Group companies.
The programme adopted in the field of Data Protection by the doValue Group aims to guarantee compliance with the applicable European and national legislation on personal data protection, to minimise the risk of any loss of confidentiality, integrity or availability, and to protect the company's information assets, made up of, to a large extent, personal data.
The Programme is kept updated according to regulatory changes and evolutions of the business context, the risk scenario and technologies.
As part of this programme, specific technical and organisational measures have been defined and implemented with a view to managing the regulatory requirements, the results of which are summarised below:

- **Record of processing activities** – Each Group company has mapped all personal data processing activities carried out, so as to distribute the roles and responsibilities correctly, to analyse the risks to rights and fundamental freedoms and to guarantee the effective exercise of those rights (on point *see* para. 1.1.4);
- **Data protection organisation model**- the effectiveness of the protection measures depends upon an adequate organisation model of the roles in charge of governing operations performed on personal data, roles of supervision (such as the Data Protection Officer), and roles of guarantee. doValue has updated its organisation model and appointed the Data Protection Officer for all Group Companies (see the next paragraph for further information);
- **Privacy policies** – all documentation aimed at guaranteeing the transparency of processing activities carried out by the Group has been updated to meet the new requirements of the GDPR, allowing the data subjects to be fully aware of the purposes of the processing activities carried out, of the other mandatory information, and of how to exercise their rights;
- **Risk analysis and impact assessment (DPIA)** – doValue has developed and adopted a new risk analysis and impact assessment to be applied to the processing activities contained in the record, in order to identify further protection measures based upon the potential material and immaterial damages that data processing may involve for the data subjects;
- **Policies & Procedures** – implementation of policies and procedures to respond to the obligations and requirements defined by the GDPR and by the other laws in that regard, including:
    - Data Protection Policy of the doValue Group
    - Procedure for managing security breaches and respective register;
    - Procedure for managing rights of the data subjects;
    - Data storage and erasure policy;
    - Privacy by design and by default guidelines;

  - Data Protection Control Framework of the DPO
- **Cyber Security Programme** – From the technical perspective, the doValue Group has defined and adopted a pervasive and robust Cyber Security programme that impacts all dimensions of governance and use of electronic tools appropriately identified to support/protect the personal data held by the Group, both as Processor and as Controller of the same.

1.1.3 Data Protection Officer

The doValue Group, in line with internal assessments and its organisational requirements, has identified and appointed a Global DPO who, at Corporate level, operates at the Parent Company doValue S.p.A.
Local DPOs have been identified in the Italian and foreign subsidiary companies who have the same role and the same responsibilities envisaged by the applicable regulations at the local level.
If a doValue Group company is not obliged to appoint its own Local DPO, the activities related to personal data protection are monitored by the Compliance or Legal Departments present locally or by another internal structure.
In order to guarantee greater effectiveness of the action of each DPO, the doValue Group has defined a *Data Protection Control Framework* ("DPCF"), which includes control activities on key areas subject to periodic monitoring. On a regular basis, each DPO assesses the adequacy and effective functioning of the controls adopted to protect personal data processing and brings the results to the attention of the company control and governance bodies in order to update the continuous improvement plan of the data protection system.
For further information on the hierarchical positioning of the DPO, on the duties attributed and on the relationships between the Global DPO, the Local DPO and the corporate control bodies, see the document *Policy Data Protection of the doValue Group*

1.1.4 Management of rights of the data subjects

In conformity with the provisions of the GDPR, the doValue Group guarantees the following rights for the Data Subjects (defined by the GDPR in Articles 15-21):

- ✓ *Right of access*: the Data Subject shall have the right to obtain confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the said personal data;
- ✓ *Right to rectification*: the Data Subject shall have the right to obtain the rectification of inaccurate personal data concerning him or her or the right to have incomplete personal data completed, taking into account the purposes of the processing;
- ✓ *Right to erasure*: the Data Subject shall have the right to request and obtain the erasure of personal data concerning him or her. Certain data, the retention of which is justified or rendered necessary for legal purposes, may not be erased (e.g. if a customer requests erasure but litigation is ongoing between him or her and the company, the latter is legitimated to store the customer's data in spite of the request);
- ✓ *Right to restriction of processing*: the Data Subject shall have the right to obtain restriction of processing if the accuracy of the personal data is contested by the data subject, for a period enabling the Controller to verify accuracy of the personal data,

or the Data Subject has objected to processing, pending the verification whether the legitimate grounds of the Controller override those of the Data Subject;

- ✓ *Right to data portability*: the Data Subject shall have the right to receive the personal data concerning him or her, in a structured, commonly used and machine-readable format and have the right to transmit those data to another Controller without hindrance;
- ✓ *Right to object*: the Data Subject shall have the right to object at any time to processing of personal data concerning him or her for some or for all the purposes for which they were collected. The Data Subject has, in particular, the right to change the consents and subsequently prevent any operation or set of operations, carried out even without using electronic tools, concerning the collection, recording, organisation, storage, consultation, processing, adaptation or alteration, selection, extraction, comparison, use, interconnection, block, disclosure, dissemination, erasure and destruction of data, even if not recorded in a database;
- ✓ *Right not to be subject to a decision based on automated processing*: the Data Subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which generates legal effects concerning him or her or similarly significantly affects him or her.

For each of the above rights, the doValue Group Companies, in the capacity of Controllers, have established appropriate internal procedures and tools to:

- provide a response to the Data Subject on the request received without undue delay, justifying to the Data Subject any delays or non-fulfilments in providing the response
- manage the requests of the Data Subject within the corporate context, executing any extraction, rectification or erasure activities of the personal data;
- inform any third party Controllers, to which the data have been communicated, of the Data Subject's request.

The Group Companies must respond to the exercise of rights by the Data Subjects whose data are processed in the capacity of Controller or in the capacity of processors where expressly requested by the Controller in the Data Protection Agreement (DPA).
In conformity with the provisions of the GDPR, the Local DPO of each doValue group company acts as a contact person for the Data Subjects in exercising their rights.
This is without prejudice in any case to the right to lodge a complaint with the Italian Data Protection Authority.
For processing activities based upon the consent of the user, the latter may withdraw consent at any time. However, the withdrawal of consent will not prejudice the lawfulness of the processing activities carried out up until that time.

1.2 CYBER SECURITY PROGRAMME

As highlighted by the *"The Global Risks Report"* of the World Economic Forum[1], the cyber risk constitutes one of the main risks for all international organisations.
The doValue Group is exposed to that risk due to the number of operators, the extensive use of electronic tools for providing services, and the nature and volumes of data processed.

1 See: http://reports.weforum.org/global-risks-report-2020/wild-wide-web/

Furthermore, the growing demand for reliability and compliance with specific requirements by the major customers of the doValue Group, the new business models that have created a context in which data and information are widely shared and interconnected, the sophistication, speed and impact of cyber attacks have all led to an increase in the complexity level of cyber risk management.
The doValue Group, through a vast Cyber Security Risk Assessment which involved all resources and systems of the Group, according to the standards ISO:IEC 27001:2015, ISO:IEC 22301:2019, NIST 800-53 and the "General Data Protection Regulation" or GDPR, defined and initiated an extensive **Cyber Security Programme**, which aims to increase the Group's security posture to the highest standards of international security and to align/transfer the security technologies chosen to all companies of the same, in a synergy-based approach.
The Cyber Security strategy defined at Group level, in particular, establishes different objectives aimed at minimising the cyber risk and therefore protecting customers, persons and the doValue brand at international level.
The objectives and results of the Cyber Security Roadmap were grouped by functions of the international Security Framework NIST, including:

- **Internal Objective 1 – Identify**
    a. Governance and risk management, supervision of the Group's critical processes through a cyber-security risk based approach;
    b. Management of the cyber risk of its supply chain;
    c. Approach oriented towards continuous improvement of the capabilities of its internal resources.

To achieve these results, the doValue Group will continue to develop its governance and risk management through:
• The definition of a Risk Appetite in support of the risk-based decision-making process;
• The use of enhanced reporting systems to support effective supervision of the programme;
• The definition of clear roles and responsibilities;
• The assessment of the risk relating to the Group's Supply Chain throughout the whole supply life cycle;
• The acquisition of internal and external resources having vertical Cyber Security skills, in order to satisfy present and future requirements in terms of cyber security.

- **Internal Objective 2 – Protect**
    a. Manage the access to resources and systems in an effective way, limited to authorised users, according to the key principles of least privilege and need to know;
    b. Identification of vulnerabilities and appropriate mitigations, promptly assessing their impact;
    c. Appropriate classification of data according to the risk exposure level;
    d. Raising of employee awareness levels through Cyber Security courses.

To achieve these expected results, the doValue Group will:
• Automate the management of identities and accesses, through a technological tool that will guarantee centralised control;
• Expand the perimeter of the security testing programme with a view to measuring, in terms of effectiveness, the IT defences and therefore protection against the intrinsic

vulnerabilities of the software and systems, which are ascertained in accordance with modern security standards;
• Improve the processes and tools for classifying sensitive data and the measures to prevent and detect the loss of the same;
• Extend the current cyber security awareness-raising programme of the doValue Group, including precise Phishing Assessment activities in order to raise the awareness of its employees regarding certain types of external attacks;
• Make the security processes more efficient through new generation services, such as centralised management of firewalls, to improve the resilience and security of all environments (BRE - Business Recovery Enhancement).

- **Internal Objective 3 – Protect**
    a. Prompt identification and management of cyber attacks;
    b. Continuous monitoring of system configurations to identify any misconfigurations;
    c. Adoption of an Event Management and Threat Intelligence system to identify in advance any Security incidents that may compromise the integrity, confidentiality and availability of the data, as well as damage the Group's reputation.

To achieve these expected results, the doValue Group will:
• implement new generation security tools and monitoring processes, in order to identify *real time* malicious activities and to understand the potential impact of the events;
• regularly carry out cyber security tests to assess the effectiveness of the cyber defences;
• strengthen the processes and procedures for detecting incidents and any compromising of the systems, based on extensive and in-depth control of the endpoints;
• make more robust the hardening process of the systems, continuously monitoring changes to the configuration with respect to the Group's Cyber Security Policy;
• activate a threat intelligence and early warning service aimed at proactively identifying threats to be able to detect malicious activities.

- **Internal Objective 4 – Respond**
    a. Regularly test the defence and incident response plans;
    b. Guarantee the response to incidents with 24x7 automated availability, where possible;
    c. Carry out forensic analysis after security incidents;
    d. Involve internal and external stakeholders in the Incident Response activities.

To achieve these expected results, the doValue Group will:
• increase the frequency of the tests of response plans to guarantee the necessary capacities and established response times, also considering the third parties involved;
• improve the tools and processes to reduce the impact of a cyber security incident, seeking to automate the response;
• implement effective processes and tools that allow technical and IT experts to carry out rigorous investigations.

- **Internal Objective 5 – Recovery**
    a. Tests and continuous improvement of the recovery plans;
    b. Guarantee that the recovery procedures from Cyber Security Incidents are carried out within appropriate predetermined timescales, respecting the

business continuity objectives (RTO, MTPD, etc) and communications to internal and external stakeholders.

To achieve these expected results, the doValue Group will:

• Regularly test the Recovery plans together with the Third Parties involved, in order to verify their effectiveness and to improve the plans in a Continuous Improvement approach;

• manage cyber security problems efficiently through coordination and communication with all interested parties, using the processes and automatisms implemented to verify the effectiveness of the response plans, mainly for ransomware and DDoS type attacks.

DoValue adopts a proactive approach towards Cyber Security, to ensure advance identification of the threat agents that could compromise in any way the Confidentiality, Integrity and Availability of the data forming part of the company's information assets, thereby facilitating, thanks to an AGILE method of management, the prompt avoidance of all pitfalls that the cyberspace entails, continuously adapting to new threats.