Document Type: *Policy*

Privacy Policy

illimity
BANCA OLTRE LA FORMA

Summary

1 PURPOSE AND SCOPE OF APPLICATION 8
2 GLOSSARY 8
3 GENERAL PRINCIPLES OF PERSONAL DATA PROCESSING 13
4 ROLES AND RESPONSIBILITIES 14
4.1 DATA CONTROLLLER 14
4.2 JOINT CONTROLLERS AND AUTONOMOUS CONTROLLERS 15
4.3 EXTERNAL PROCESSORS 15
4.3.1 EXTERNAL PROCESSORS APPOINTED BY THE BANK 15
4.3.2 ROLE OF EXTERNAL PROCESSOR DEPLOYED BY THE BANK 16
4.4 SUB-PROCESSORS 16
4.5 DATA PROTECTION OFFICER (DPO) 16
4.5.1 OPERATING MANUAL OF THE DPO 17
4.6 PRIVACY OFFICER 18
4.7 PROCESSORS 19
4.8 SYSTEM ADMINISTRATORS 20
4.9 SINGLE POINTS OF CONTACT (SPoCs) 20
5 PROCESSING OF PERSONAL DATA 20
5.1 LEGAL BASES FOR PROCESSING 20
5.2 TYPES OF DATA PROCESSED AND MEANS OF PROCESSING 20
5.3 CATEGORIES OF DATA SUBJECTS 21
5.3.1 EMPLOYEES, FORMER EMPLOYEES, COLLABORATORS/INTERNS, CANDIDATES AND MEMBERS OF CORPORATE BODIES 21
5.3.2 CUSTOMERS AND PROSPECTIVE CUSTOMERS 21
5.3.3 USERS OF THE WEBSITE 22
5.3.4 SUPPLIERS, POTENTIAL SUPPLIERS AND THIRD PARTIES 22
5.3.5 NATURAL PERSONS ASSOCIATED WITH LEGAL PERSONS WITH WHOM THE BANK HAS A BUSINESS RELATIONSHIP 23
5.4 PROTECTION AND SECURITY MEASURES 23
5.5 PROCESSING REGISTER 23
5.6 RETENTION AND ERASURE OF DATA 24
6 INFORMATION AND CONSENT TO THE PROCESSING OF DATA 30
6.1 INFORMATION 30
6.2 CONSENT 30
7 MANAGING THE RIGHTS OF DATA SUBJECTS ON DATA PROCESSING MATTERS 31
7.1 RIGHTS OF THE DATA SUBJECT 31
7.1.1 RIGHT TO ERASURE 31
7.1.2 RIGHT TO ACCESS 31
7.1.3 RIGHT TO RECTIFICATION 32
7.1.4 RIGHT TO OBJECT 32

7.1.5 RIGHT TO RESTRICTION ... 32
7.1.6 RIGHT TO DATA PORTABILITY ... 32
7.1.7 RIGHT NOT TO BE SUBJECT TO A DECISION BASED SOLELY ON AUTOMATED PROCESSING ... 33
7.1.8 RIGHT TO LODGE A COMPLAINT WITH THE SUPERVISORY AUTHORITY ... 33
7.2 MANAGING THE REQUESTS OF DATA SUBJECTS ... 33
7.2.1 TIME PERIODS FOR MANAGING THE REQUESTS OF DATA SUBJECTS ... 33
7.2.2 RECEIPT OF THE REQUEST ... 33
7.2.3 RECORDING THE REQUEST ... 34
7.2.4 FORMAL ASSESSMENT OF THE REQUEST ... 34
7.2.5 ASSESSMENT OF THE MERITS OF THE REQUEST AND DESPATCH OF THE RESPONSE TO THE DATA SUBJECT ... 34
8 DATA PROTECTION IMPACT ASSESSMENT (DPIA) ... 36
8.1 DATA PROTECTION IMPACT ASSESSMENT ... 36
8.2 REQUIREMENTS FOR PERFORMING A DPIA ... 38
8.3 IMPACT ASSESSMENT PROCEDURE ... 39
8.3.1 STAGE 1: DETERMINE THE CONTEXT AND OBTAIN AN OVERVIEW OF THE PROCESSING IN QUESTION ... 39
8.3.2 STAGE 2: BASIC PRINCIPLES ... 39
8.3.3 STAGE 3: RISKS ... 40
8.3.4 FASE 4: ACTION PLAN ... 40
9 DATA BREACHES ... 41
9.1 SCOPE OF APPLICATION ... 41
9.2 ROLES AND RESPONSIBILITIES IN MANAGING DATA BREACHES ... 41
9.2.1 DATA CONTROLLER ... 41
9.2.2 DATA PROTECTION OFFICER (DPO) ... 42
9.2.3 COMPLIANCE & AML ... 42
9.2.4 DATA BREACH MANAGEMENT GROUP ... 42
9.2.5 STRUTTURES INVOLVED IN THE PROCESS ... 42
9.3 PROCEDURE FOR MANAGING A DATA BREACH ... 42
9.3.1 STAGE 1: DETECTING AND REPORTING A PERSONAL DATA BREACH EVENT ... 42
9.3.2 STAGE 2: ANALYSIS, CLASSIFICATION AND RECORDING OF A PERSONAL DATA BREACH INCIDENT ... 43
9.3.3 STAGE 3: NOTIFICATION AND COMMUNICATION OF A DATA BREACH ... 45
9.3.4 STAGE 4: CLOSING A PERSONAL DATA BREACH INCIDENT ... 46
10 TRAINING OF STAFF INVOLVED IN PERSONAL DATA PROCESSING ... 47
11 PRIVACY CONTENTS OF THE BANK'S WEBSITE ... 47
11.1 PRIVACY SECTION: CONTENTS AND UPDATING ... 47
11.2 COOKIE POLICY SECTION: CONTENTS AND UPDATING ... 47
12 ANNEXES ... 48
12.1 ANNEX 1: INTERNAL RELATED REGULATIONS ... 48

12.2 ANNEX 2: EXTERNAL RELATED LEGISLATION AND REGULATIONS 48

12.3 ANNEX 3: PROCESS OF MANAGING REQUESTS FOR EXERCISING THE RIGHT OF ERASURE OF PERSONAL DATA 49

12.4 ANNEX 4: PROCESS OF MANAGING REQUESTS FOR EXERCISING THE OTHER RIGHTS OF DATA SUBJECTS 52

12.5 ALLEGATO 5: FACSIMILE FOR INFORMING THE CORPORATE BODIES OF A DATA BREACH 54

This Policy establishes the principles underlying the processing of personal data carried out by illimity Bank S.p.A. – at the level of business line and technical/operating and organisational support structures – and describes the processes and procedures governing the performance of all the associated activities.

The Policy also identifies the roles and responsibilities within the organisation adopted by the Bank – whose management is represented by the Group's Data Protection Officer (DPO) – as a means of presiding over the issues and legislative and regulatory obligations on the processing of personal data, in compliance with the applicable requirements of national and European Union law as well as the decisions and provisions issued from time to time by the Italian Data Protection Authority.

The principles and guidelines contained in this document are applicable to the Bank and all the companies of the Banking Group subject to the management and coordination of the Parent Company, for the parts of respective competence and depending on the nature of the activity performed by each individual subsidiary. Group companies are accordingly required to include the contents of this Policy in their own internal rules and regulations on the matter (suitably tailored for their individual processing specifics).

This Policy sets out the regulatory framework which all members of the Bank's staff are required to know and fully apply in performing their individual job responsibilities, also satisfying their duty to keep updated and follow diligently and consciously the training and information sessions on privacy laws and regulations organised by the Bank on the security measures and risks inherent in the processing activities performed. The staff involved in personal data processing activities are constantly updated on the requirements and forms of conduct to be followed, in particular by way of:

- the dissemination of information referring to laws and regulations, also internal, both in the general aspects and in key individual situations;
- specific training courses;
- sending out suitable training "nuggets" designed to explain in a simple and immediate way the aspects of the most important laws and regulations in the ambit of the daily activities performed by the personnel of the various functions.

Failure to comply with the rules and regulations described in this Policy represents personnel conduct subject to disciplinary measures, in accordance with the relative human resources management processes.

In addition, the contents of this Policy govern both processing performed by the Bank as data controller and that carried out by the Bank as external processor acting on behalf of third party data controllers (where relevant). In the same way, the Policy governs the characteristics of the processing performed by third parties appointed by the Bank as external processors, which are instructed to carry out specific activities as part of service agreements. Such external processors are provided with specific instructions designed to ensure compliance with this document and with privacy laws and regulations as well as to provide adequate protection of the data being processed, in accordance with the standards and minimum measures adopted by illimity.

In application of the above-mentioned laws and regulations on privacy, the Bank guarantees that it will carry out processing in compliance with the fundamental principles of loyalty, fairness and minimisation as well as judicial bases relevant from a legislative and regulatory standpoint. To this end, the Policy describes the macro-types of processing performed by the Bank as part of ordinary operations and specifies their purposes, providing details of the categories of data and the data subjects involved as well as the established retention terms.

The document also sets out the roles and responsibilities of the various players involved in managing privacy issues and detailing the various internal processes, with particular reference to the role of the Data Protection Officer - DPO appointed by the Bank and the figures identified to support him in the practical work involved (specialist staff assigned to manage operating activities). In any case, all members of the Bank's staff are involved in adopting the most appropriate technical and organisational measures for ensuring the accuracy and protection of the data processing carried out. To this end, this Policy also describes the duties of the other parties involved in managing privacy matters, namely the Single Points of Contact ("SPoCs") identified within the various business areas of the Bank, whose duty is to ensure the accuracy and constant updating of all the information and characteristics of the processing performed within their respective fields of competence/responsibility as well as guaranteeing that such are appropriately recorded in the processing register that the Bank is required to keep.

In addition, the Policy provides a description of the Bank's methodology for assessing the impact of data protection (the "Data Protection Impact Assessment") regarding the processing most exposed to risk, in accordance with the most accredited international standards on the matter.

Lastly, the document describes the internal procedure for managing personal data breaches – and the model for assessing the gravity of the breach – as well as the processes for a proper management of the requests made by data subjects to exercise their rights, in accordance with the applicable legislative and regulatory requirements.