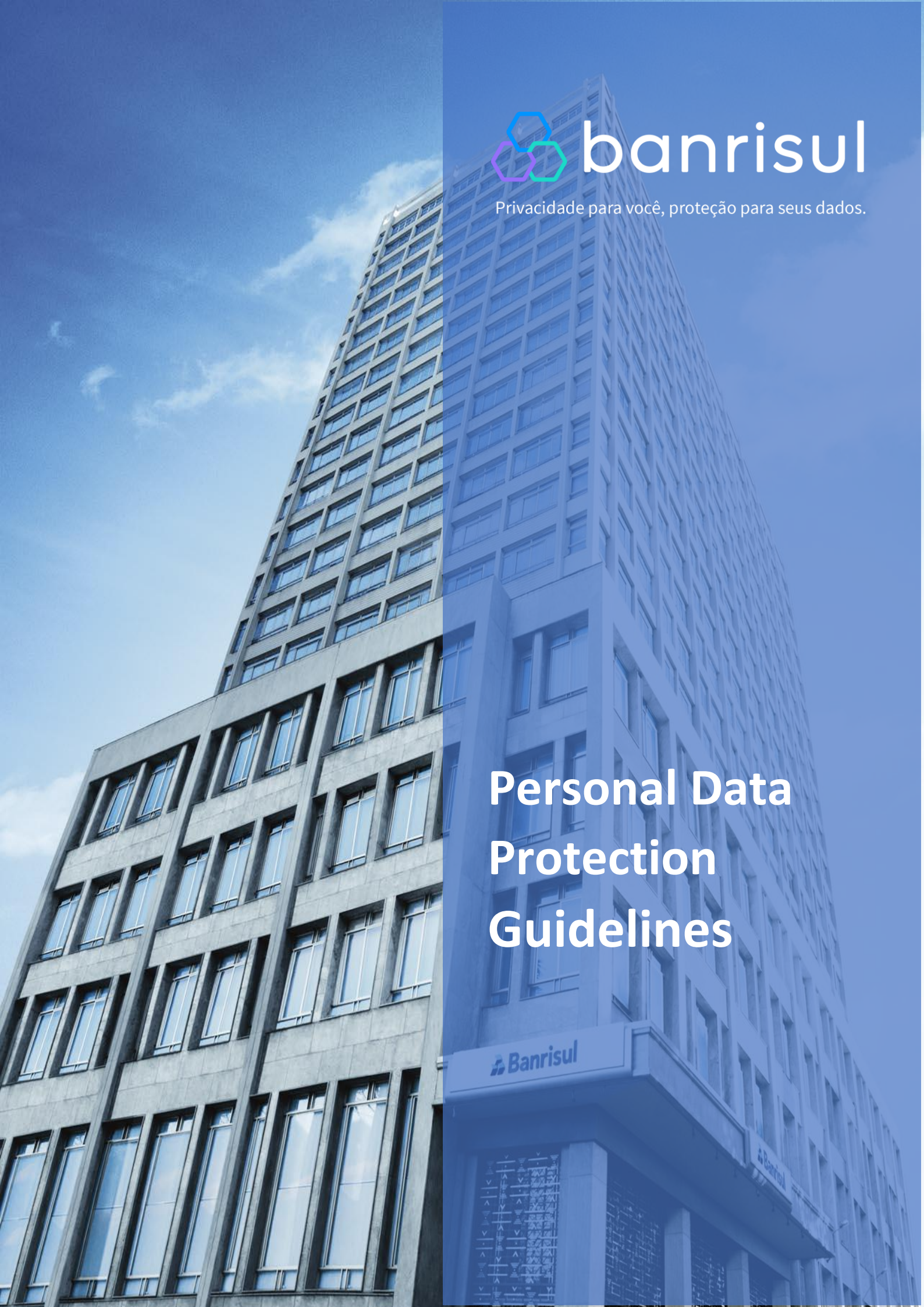
banrisul
Privacidade para você, proteção para seus dados.
Personal Data Protection Guidelines
Banrisul

Personal Data Protection Guidelines

Context

Banrisul, directly or through its representatives, employees, or suppliers, carries out several Personal Data Processing operations. With the General Data Protection Law (Law 13,709/18, or "GDPR") coming into effect, we must ensure that these operations are in line with legal requirements and best practices for the protection of Personal Data.

The enactment of Constitutional Amendment 115, in February 2022, recognized the importance of protecting personal data in Brazil and includes the fundamental rights and guarantees of the Brazilian Federal Constitution.

Therefore, as a way to signal its institutional commitment to the fundamental rights to privacy and the protection of Personal Data, Banrisul presents below the Guidelines for the Protection of Personal Data.

Purpose

These Personal Data Protection Guidelines establish principles, rules, attributions, and responsibilities to ensure Banrisul's compliance with the GDPR.

Banrisul declares, through these Guidelines, its commitment to maintaining the balance between its economic interests and the protection of Data of Personal Data Holders, including clients, business partners, and employees.

Scope and Target Audience

These Guidelines apply to:

Banrisul's Employees, Administrators, Board Members, Members of Statutory and Advisory Committees to the Executive Board, Interns, and other Collaborators.

All of Banrisul's current subsidiaries, namely Banrisul Soluções em Pagamento S.A., Banrisul S.A. Administradora de Consórcios, Banrisul S.A. Corretora de Valores Mobiliários e Câmbio, Banrisul Seguridade Participações S.A., Banrisul Corretora de Seguros S.A., and Banrisul Armazéns Gerais S.A.

Banrisul's Suppliers, Service Providers, Partners, and their respective Agents and Employees, referred to herein as "Third Party" or "Third Parties", who, within the scope of their contracts, carry out the Processing of Personal Data owned by the Bank or the Bank's clients due to joint activities conducted with the Bank, as Processing Agents.

Principles to be Observed

Responsibility and Accountability

Processing Agents (Controller and Operator) must demonstrate they adopt measures and procedures to protect Personal Data during the Data Processing life cycle.

Privacy and Data Protection Culture

Actions must be created to raise the awareness of all parties related to Banrisul, including employees, clients, and/or third parties, regarding the commitment of the Bank to the proper protection of the Personal Data of these related parties and the enforcement of their rights as Data Holders.

Purpose and Suitability

The Processing of Personal Data must be carried out for a legitimate and specific purpose, compatible with the purposes informed to the Holder, under the context of the Processing activities.

Requirements

Data must receive the minimum Processing required to fulfill its purpose, without excessive Data.

Quality, Free Access, and Transparency

Data Holders must have access to clear, precise, and easily available information about the Processing of their Personal Data, which must be correct and up-to-date.

Safety and Prevention

Technical and administrative measures must be adopted to protect Personal Data and prevent incidents from occurring.

Non-discrimination

Processing cannot be carried out for discriminatory, illegal, or abusive purposes.

Processing of Personal Data at Banrisul

Any and all Processing of Personal Data carried out by, or on behalf of, Banrisul must have a legitimate and specific purpose and must be supported by, at least, one of the legal hypotheses provided in articles 7 or 11 of the GDPR. Additionally, no Personal Data should be processed differently than what was informed to the Holder of the Personal Data.

Efforts must be made to ensure that Personal Data Holders are properly informed about the Processing of their Personal Data. If Personal Data is shared with third parties (including those belonging to the same economic group), Banrisul shall guarantee Data Holders, as requested, access to clear, concrete, and wide information about the sharing, including its respective purpose.

Banrisul's Privacy Policy provides information necessary for Data Holders to gain awareness of the Processing activities it carries out, as well as the channels available for the Holders to exercise their rights provided in the GDPR.

Processing of Data on Children and Adolescents

The processing of Personal Data belonging to children and adolescents must be carried out with maximum caution and always in their best interest, to be assessed in the specific case, under article 14 of the Law.

According to the understanding of the National Data Protection Authority ("ANPD") in Brazil, the Processing of Personal Data of children and adolescents can be based on any of the hypotheses provided in articles 7 and 11 of the GDPR, provided that their best interests prevail, including cases where the consent of parents or legal guardians is applicable. When the data of children and adolescents are processed with the collection of consent from the responsible party, such consent must be explicit, specific, and prominent, and the purpose to be fulfilled by the Processing must be indicated.

Processing of Personal Data by Third Parties

Before signing any relationship/agreement with Third Parties that requires the Processing of Personal Data, the parties involved must be instructed to gain awareness of Banrisul's Personal Data Protection Guidelines and its Privacy Policy, available on the Bank's website, and to comply with the applicable data protection rules, notably the GDPR.

The rules and requirements for contracts and/or relationships involving the sharing of Personal Data shall be included in the clauses of the respective contracts, amendments, and/or declaration terms, observing the peculiarities and nature of each negotiation relationship and, whenever possible, pseudonymous data and other techniques will be used to guarantee the confidentiality of the Data.

If Personal Data is shared with other entities, Banrisul shall guarantee Data Holders, as requested, access to clear, concrete, and wide information about the sharing of information, including its respective purpose.

Non-compliance with any of the requirements must be documented and liabilities may be created on behalf of the Third Party, within the context of the respective contract/relationship, exempting Banrisul from any charges.

Safety Measures and Good Practices

In line with good practices and in compliance with legislation, Banrisul adopts security, technical, and administrative measures aiming to protect Personal Data against unauthorized access, accidental or intentional manipulation, loss, and destruction.

Personal Data processed at Banrisul are only transmitted when necessary and through secure connections. Data referring to passwords stored in Banrisul's Databases are encrypted with algorithms that guarantee a high level of security.

The granting of access to Personal Data processed by Banrisul is restricted to authorized employees who need to Process such Data to perform their duties at the Company, observing the principles of purpose, adequacy, necessity, and transparency.

The storage period for collected Personal Data relies on the purpose and nature of the Processing that is being carried out. We will maintain collected Personal Data during the period required to comply with legal and/or regulatory and contractual obligations, to continue to provide and enhance our products and services, for risk management purposes, for the common exercise of rights in administrative and judicial proceedings, and for the other purposes outlined herein.

Security Incidents

Based on current regulations and best market practices, the Guidelines for the Prevention and Response to Incidents with Personal Data at Banrisul establish specific control procedures aimed at preventing and addressing incidents, including processes designed to prevent incidents that may pose a significant risk or harm to data holders.

Rights of Personal Data Holders

Personal Data Holders, upon formal request and through specific channels, may obtain information on their own Personal Data.

At Banrisul, the Person in Charge – also known as the "Data Protection Officer" (DPO) will act as an interlocutor and communication channel between the Controller (Banrisul), the Data Holders, and the National Data Protection Authority (ANPD).

International Transfer of Data

In exceptional cases where there is a need to transfer personal data to foreign jurisdictions, Banrisul ensures that such transactions are carried out only when there are adequate protection guarantees, including standard contractual clauses and privacy certifications.

Update

The Personal Data Protection Guidelines will be reviewed at least once a year to ensure they are up-to-date, aligned with current legislation and regulations, and in line with good market practices and/or may also be reviewed upon recommendations from Senior Management.

Glossary

The terms used in the Data Management Policy, Data Governance Program, and Personal Data Protection Guidelines at Banrisul, when capitalized, shall have the definitions and concepts[1] provided below:

General

Data: all Data and information represented by characters, texts, numbers, images, sounds, trademarks, or videos, whether internal or external to the institution.

Open Data: Those accessible to the public, represented in digital format, structured in an open format, machine-processable, referenced on the Internet, and made available under a license that allows their free use, consumption, or cross-referencing, limited to crediting the authorship or source.

[1] [1]The concepts and terms used in this policy are based on the Data Management Body of Knowledge (DAMA DMBOK®), a best practice framework aimed at emphasizing the importance of Data Management in organizations, and the terms introduced by the General Data Protection Regulation - GDPR.

Corporate Data: all Data and information represented by characters, texts, numbers, images, sounds, trademarks, or videos, related to Banrisul and managed within the institution.

Data Steward: Units/bodies responsible for managing a specific set of Data originating from their business processes, represented by their leaders (superintendents and executive managers) involved in the strategy and business processes under their responsibility.

Data Governance

Use Cases: describe how Data will be used for information, both for internal purposes and to meet external demands, representing opportunities for data-driven decision-making.

Corporate Data Catalog (Catalog): seeks to gather de definitions, rules, and uses of data generated in various Banrisul processes so that they can be shared among organizational units. The Catalog is designed to help users understand the business language and the meaning of information assets.

Data Curator: employee(s) who know the concepts, uses, and sharing of Data generated and managed in the administrative units/bodies in which they operate and are responsible for conducting, in their area, the methodology for cataloging and qualifying Data, together with the Data and Analytics Management Unit.

Derived Data: Data calculated from other domains, performs Data transformation and information reporting.

Reference Data: Static data used as a reference for a transaction, with cross-business use.

Transactional Data: Data exclusively related to the transaction, with a direct financial impact on the Bank and aligned with the products of the business unit.

Data Marts: a subset of Corporate Databases, with different levels of aggregation, built from the Data elements defined with the managing units and aimed at meeting their usage needs, which can generate corporate views.

Business Dictionary: a set of Metadata that defines the context of Data Elements - their conceptual business definition, uses and purposes, and quality monitoring rules.

Technical Dictionary: a set of technical Metadata of Data Elements, including the identification of their physical representation and Data Lineage.

Domain: areas of Banrisul separated by subjects, which are responsible for managing Data that can be transactional, reference, or derived.

Data Element: Data that obeys a unique concept, described in its smallest granularity, regardless of its physical representation (table, file, system, etc.).

ETL: Extract, Transform, Load is the process that involves extracting Data from various external sources; transforming Data to meet business needs; and loading Data. ETL is how data is extracted and loaded into the Corporate Database. The IT team uses IBM InfoSphere DataStage for ETL processes.

Data Lineage: it is the life cycle of Data, describing where it originates, where it passes through, and where it is stored. Data Lineage also allows the traceability of specific data sources for the identification of errors and improvements in flows and interfaces.

Metadata: contextualized Data that describes, explains, locates, or facilitates the use of data, turning it into information. They are often referred to as “data about data”.

Modelers: the primary employees responsible for creating reports and dashboards - those who access data, create panels, and make them available to other internal users within the units/network.

Quality (Monitoring) Rules: sets of criteria or conditions that can qualify data in terms of reliability. The rules are defined by the Data Steward and Curators, and implemented with the guidance and support of the Data and Analytics Management and Systems Development teams, with their incorporation into the Data Stage tool (IBM InfoSphere).

Self-Service Analytics: an advanced analysis method that allows business professionals to work independently through self-service. The use of self-service tools on organized tables, with standard and consistent structure and nomenclature (Data Marts), enables professionals to quickly and intuitively manipulate Data in search of new business opportunities (insights).

Staging Area: a preparation and temporary storage area used for Data processing during the extraction, transformation, and loading (ETL) process. It sits between the source systems and the Data’s ultimate destination, the Corporate Database.

Quality Tests: defined based on the rules mapped and established by the managing units. After implementing the rules, each record is tested when loaded, and this process generates alerts and reports according to the frequency and format defined during implementation.

***Tombamento*:** internal methodology aimed at safeguarding and preserving data by implementing mechanisms and processes that qualify and disseminate the importance of these assets for the organization's business.

Protection and Privacy of Personal Data

Processing Agents: the Controller and Operator who carry out the Processing of Personal Data.

National Data Protection Authority: the indirect public administration body responsible for ensuring, implementing, and supervising compliance with the GDPR.

Consent: the free, informed, and unquestionable manifestation by which Data Holders agree with the Processing of their Personal Data for a specific purpose.

Controller: a natural or legal person, public or private, responsible for decisions regarding the Processing of Personal Data.

Anonymous Data: Data relating to Data Holders who cannot be identified, considering the use of reasonable technical means available when the data is processed.

Pseudonymous Data: a protection technique by which layers are added to Personal Data, in such a way that only the controller can identify the person because it is the only party that holds additional information about a determined or determinable individual.

Personal Data: any information relating to an identified or identifiable natural person.

Sensitive Personal Data: information that may reveal aspects of a person's privacy related to racial or ethnic origin, religion, political opinion, membership to unions or religious,

philosophical, or political organizations, and data concerning the health or sex life, as well as genetic or biometric data of a natural person.

Data Protection Officer: as referred to in the General Data Protection Regulation (GDPR) of the European Union, the DPO is a natural person or legal entity focused on ensuring a company's compliance with data protection standards and best practices, and respect for privacy. In Brazil, Law 13,709/18 (General Data Protection Regulation) adopted the term "*Encarregado*" (person in charge). Banrisul indicates the person who shall act as an interlocutor and communication channel between the controller (Banrisul), Data Holders, and the National Data Protection Authority (ANPD), in addition to the other activities provided in paragraph 2 of article 41 of the GDPR.

Security Incidents: an undesired or unexpected event, which is likely to compromise the security of Personal Data, in such a way they are exposed to unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication, or any other form of inappropriate or unlawful treatment.[2]

Operator: a natural or legal person, public or private, responsible for decisions Processing Personal Data on behalf of the Controller.

Privacy by Design and Privacy by Default: methodologies in which the protection of Personal Data is elaborated from the conception of systems, commercial practices, projects, products, or any other solution that involves the handling of Personal Data.

Data Protection Impact Report: a document prepared by the Controller containing the description of procedures used to process personal data that may generate risks to civil liberties and fundamental rights, as well as risk mitigation measures, safeguards, and mechanisms.

Data Holder: a natural person object of the Personal Data that is being Processed.

Processing: Any operation carried out with Data, including collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, deletion, evaluation or control of information, modification, communication, transfer, dissemination, or extraction.