Cerved Group S.p.A.

General Personal Data Protection Policy

Approved by the Board of Directors on 23 December 2019

Table of Contents

1 Objective and scope of application

1.1 OBJECTIVE

The present policy document ('**Policy'**) aims to set out the commitments undertaken and the policies implemented by Cerved Group S.p.A. ('**Cerved**') and by the companies belonging to it ('**Cerved Group**' or '**Group'**)[1] with regard to the protection of personal data, in terms of organisational matters and key roles for applying the relevant regulations in force, as well as in terms of the internal procedures, regulations and measures adopted in order to ensure compliance with the law.

All corporate bodies concerned were involved in the process of drafting and revising this Policy, which has been approved by the Cerved Board of Directors.

The Policy will be reviewed – and revised if necessary – periodically, as well as in conjunction with updates or changes to the relevant regulatory framework and its interpretation by the European Data Protection Board (**EDPB**) and/or by the Italian Data Protection Authority ('**Authority'**), or as a function of new developments within the organisation and its business activities, its corporate projects and processes, or its information technology platforms and applications in use.

This Policy shall remain available on the Cerved website (www.cerved.com), as well as publicised and made available to all personnel via the Company's intranet and on the Workplace platform, along with operational indications and other related internal documentation.

Cerved undertakes to promptly inform all parties concerned of any amendments or revisions to the Policy, by publishing any related updates without delay on the relevant web pages.

1.2 SCOPE OF APPLICATION

The present Policy applies to all Cerved Group companies.

1.3 PARTIES CONCERNED

This Policy applies to all Personal Data Processing activities carried out by the Cerved Group. It therefore applies to all bodies, functions, departments and individuals of the Group that are authorised to process personal data, as well as to all Data Processing activities carried out on behalf of Cerved Group by third parties who act as Data Processor.

[1] The updated corporate structure of the group is available at: https://company.cerved.com/en/group-structure

2 Regulatory Framework

2.1 RELEVANT LEGISLATION

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ('**GDPR**' or '**Regulation**'), in force since 25 May 2018, repealed Directive 95/46/EC of 24 October 1995, consequently rendering inapplicable all implementation legislation issued by EU Member States related to the latter Directive, at least as regards any portions not compatible or in contrast with the provisions of the GDPR.

Italy recently adjusted its national data protection regulations to the GDPR through Legislative Decree no. 101/2018 of 10 August 2018, which took effect on 19 September 2018. The pre-existing law, Legislative Decree no. 196/2003 ('**Data Protection Code**'), was overhauled under Decree no. 101/2018, with numerous paragraphs repealed, amended or supplemented.

At present, personal data protection is therefore regulated in Italy by both the GDPR and the national Personal Data Protection Code as amended by Decree 101/2018. In the business information industry, data protection is also regulated by the *Code of Conduct in the Processing of Personal Data in the Field of Business Informati*on, as submitted by industry association ANCIC (the Italian national association of business information and credit management companies) and approved by the Authority on 12 June 2019 (it will take effect upon completion of the accreditation phase by the Authority's monitoring body). Further regulations include the Authority's general provisions and guidelines on personal data, as well as provisions and guidelines issued by both the former Working Party pursuant to article 29 of Directive 95/46/CE (known as '**WP29'**) and its replacement, the aforementioned European Data Protection Board (EDPB), which provides guidance, indications, recommendations and implementation-related clarifications regarding the requirements introduced under the GDPR, all of which have been amply taken into account in preparing the present Policy.

A glossary provided at the end of the present document defines the key terms used herein, in line with the regulations in force; the glossary is followed by two appendixes, the first on the main compliance requirements and the second on the new requirements introduced under the GDPR which Cerved Group and its companies are committed to following in order to guarantee that all activities are compliant with this Regulation.

3 Roles, duties and responsibilities for personal data protection

Cerved, as a Data Controller, has established specific roles and responsibilities to ensure that the new organisational model will be directed, governed, executed and monitored with a view to protecting personal data.

3.1 CORPORATE BODIES, FUNCTIONS, DEPARTMENTS AND BUSINESS UNITS

3.1.1 Board of Directors

The Board of Directors, in its capacity as Cerved's governing body, has delegated the main powers of planning, managing and monitoring data protection obligations to the Chief Executive Officer. The Board has also assigned the title of 'Data Protection Delegate' to the current managers of certain company departments that report directly to the governing body, within the limits of powers already assigned to these managers; this role entails responsibility for specific functions related to applying personal data protection regulations, including allocating the relevant tasks and duties in order to ensure appropriate execution and management of Personal Data Processing activities in their respective departments for compliance with GDPR requirements.

3.1.2 Privacy Delegates

The Privacy Delegates described above shall receive applicable information and suitable guideline updates on data protection matters. Delegates may appoint one or more colleagues within their respective department or unit as 'Privacy Contacts' (see point 3.1.3 below) to support them in carrying out their function of applying data protection regulations. Each Data Protection Delegate will be called upon to manage, coordinate and monitor the Personal Data Processing activities conducted within the Delegate's respective department or unit, along with the related GDPR compliance obligations relevant to that department or unit. The Delegate's role includes the power to supervise the implementation of all technical and organisational actions and measures necessary pursuant to articles 24 and 32 of the GDPR, in order to enable the Data Controller to guarantee and to be able to demonstrate that all personal data has been processed in accordance with the laws in force, taking a proactive approach to sustaining effective use of and adherence to the policies, procedures and guidelines adopted by the Cerved Group for the purpose of compliance with the GDPR.

3.1.3 Privacy Contacts

Cerved Group has envisaged assigning the role of Privacy Contacts to some individuals who are authorised to process personal data. These Privacy Contacts attend specific training sessions

about personal Data Processing regulations and must fulfil a safeguarding role in order to establish observance of the principle of accountability, through active cooperation with a view to concretely following and implementing the procedures and guidelines adopted by the Cerved Group for the purpose of GDPR compliance (with particular reference to keeping records of processing pursuant to article 30 of the GDPR, to conducting associated risk analysis, to the *Data Protection Impact Assessment Procedure*, the *Guidelines for Data Protection By Design and By Default*, and the *Procedure for Handling Personal Data Breaches*).

Privacy Contacts are responsible for ensuring that all persons authorised to process data who are under their coordination, or with whom a working relationship has been validated by respective Privacy Delegates, adopt and follow appropriate security measures stipulated in Personal Data Processing regulations, so as to minimise the risks of: destruction or loss (even accidental) of such data; unauthorised access to the data; and processing in a manner that is not permitted or not in accordance with the purpose of the data collection activity. To this end, the Privacy Contacts must also monitor the Data Processing activities of all Authorised Persons within their respective areas of oversight (as per the Company's organisational chart) to ensure that such activities are executed appropriately and that the Authorised Persons receive and execute proper instructions on Data Processing methods and practices.

3.1.4 Data Protection Officer (DPO)

The individual appointed as Data Protection Officer (DPO) must be sufficiently autonomous and independent. The DPO must be able to provide specialised consulting on data protection issues in each of Cerved Group's business units and, at the same time, conduct generally second-level supervision of procedures, measures and documentation adopted by each unit in order to verify compliance with the GDPR, providing indications and recommendations on the matter to the relevant Cerved Group company's governing body, by reporting directly to the CEO or to another function to which the CEO or Board of Directors has delegated relevant powers, by means of periodic written reports, except for urgent cases, which must be reported without delay.

As parent company, Cerved evaluated the need to appoint a DPO based on Whereas Clause 97 and article 37 of the GDPR along with the WP29 Guidelines for data protection on data protection officers[2] and the Italian Authority's FAQ sheet for the private sector[3]; the Company decided in favour of the option – pursuant to GDPR article 37 paragraph 2 – to appoint a single DPO for all

[2] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048
[3] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8036793

Cerved Group companies, with the exception of its foreign subsidiaries, which have proceeded to appoint local DPOs.

Cerved Group has opted to assign the DPO function to an individual who is external to the organisation, following a selection process to identify a candidate possessing the requirements stipulated in the GDPR for the role of DPO for the entire group of companies; the selection process involved specific verification that the individual possesses specific expert knowledge and professional qualities as per article 37 paragraph 5 of the GDPR, and furthermore that the individual has no conflict of interests with any other tasks or duties in the Cerved Group in accordance with article 38 paragraph 6 of the GDPR.

In addition, Cerved Group has identified professionals within Cerved's Legal Department who are experts on personal data protection law. These individuals can facilitate coordination between internal resources and the designated DPO, so as to provide the latter with suitable conditions for fulfilling his/her tasks more easily, as per article 38 paragraph 2 of the GDPR.

The DPO's contact information has also been provided to the Authority and published on the data protection information section of the corporate website.

3.1.5 Internal Audit

The Internal Audit function:

- verifies, on a continuous basis and in connection with specific needs in accordance with international standards, the operability and suitability of the internal audit and risk management system, through an audit plan approved by the Board of Directors based on a structured process of analysing and prioritizing the main risks;
- verifies the appropriate and effective functioning of risk management models adopted by the company, including for compliance risk, with the aim of ensuring that the models enable company management to manage risks effectively, from both a methodological and a practical point of view.

Within this context, the audit plan for the companies of the Cerved Group includes a specific aspect for "Verification of the effectiveness of monitoring practices for GDPR compliance". The plan also includes continuous verification of the Group's "information security management system", conducted in accordance with the ISO 27001:2017 standard, for the purpose of verifying whether the technical and organisational security measures adopted are adequate.

Furthermore, 'process audits' may include specific checks on the proper application of GDPR provisions (both internal and external regulations). Activities directly or indirectly connected to the GDPR are carried out in coordination with the DPO and with the Group's Privacy Executive.

3.1.6 Information Technology

The information technology (IT) department of each Cerved Group company, along with the Privacy Delegates who manages, coordinates and monitors the Personal Data Processing activities carried out in that department, must jointly perform data security risk analyses on the data computing systems and IT services of the respective Group company, in order to determine what security measures should be implemented, assess the efficacy of current measures, as well as handle and report Personal Data Breaches. The IT function must also support technical and technological aspects of data protection impact assessments (DPIAs) and support the DPO on computing matters. On behalf of the Data Controller, the IT function also manages and performs the most technical aspects involved in implementing personal data protection rules, providing specialised support, advice and monitoring where needed, with particular reference to the supervision and coordination of implementing Group and company policies on data and systems security, as well as on the analysis and assessment of the technical and technological risks associated with processing personal data, updating and monitoring IT infrastructure and technological measures in accordance with data protection regulations, and managing Personal Data Breaches as mentioned above. In addition to its responsibility for properly handling the processing of personal data acquired, registered, generated and/or stored in respective IT systems, the IT departments are also assigned specific functions concerning the assessment, planning, adoption and monitoring of the Group's data and systems security measures so as to ensure compliance with GDPR standards, based partly on the Group's own policies. The IT function also acts as a focal point for the handling and notification of potential Personal Data Breaches, wherever such violations are related to the Group's computer systems, in which where deemed necessary, prompt consultation support from the DPO may also be requested.

3.1.7 Human Resources

The Human Resources department is assigned functions pertaining to observing the GDPR provisions and national personal data protection regulations with respect to the Group's employees and workers. This department may be assigned additional tasks regarding, in general, identifying (along with relevant department or unit managers) employees and workers to authorise for Personal Data Processing and determining the scope of processing authorised to each of them, as well as establishing confidentiality guarantees and documented instructions on this matter, and finally, carrying out relevant training activities based on the requirements of the various corporate units.

3.1.8 Persons authorised to process Personal Data

Cerved Group identifies certain staff members to be authorised to process personal data within their respective departments, units or offices. These individuals operate under the direction and supervision of the relevant department head and/or Privacy Delegate. They must follow instructions received in accordance with data protection regulations and with the *Guidelines on Persons Authorised to Process Personal Data*, a document which covers the roles, obligations and instructions of such persons within the Cerved Group.

It is specifically envisaged that each newly Authorised Person receives, upon signing the related authorisation to process personal data, specific instructions on the processing tasks to be completed on behalf of Cerved Group and in connection to which the Authorised Person assumes confidentiality obligations that extend well beyond the end of the employment or supply contract. Upon authorisation to process data, these persons also receive the *Use of IT Tools Policy* document, which also remains available permanently on the corporate intranet, containing instructions to handling credentials, using e-mail and the Internet and other IT tools within the company, as well as the *Procedure for Handling Personal Data Breaches*. Finally, Cerved Group sponsors annual internal training courses led by sector experts, with the aim of raising awareness about data protection issues among authorised staff members.

3.1.9 Systems Administrators

Any person who manages and maintains Data Processing systems used to process personal data, including database management systems, complex software such as Enterprise Resource Planning (ERP) systems used in large companies and organisations, local IT networks and related security devices, on a non-occasional basis to the extent that the person could perform tasks that affect such personal data (even if occasionally) is considered, for the purpose of this Policy, to be a Systems Administrator.

Cerved Group assigns Systems Administrator duties to those who can guarantee experience, professional skills and reliability; they are individual designated as such and registered on a list with the names of all Systems Administrators. The operations performed by these individuals are subject to audit at least once a year by the Data Controller, so as to verify observance of organisational, technical and security measures regarding Personal Data Processing as per the regulations in force. Finally, Systems Administrators must adopt appropriate systems for logical registration access (authentication) to the Group's Data Processing systems and electronic archives.

3.1.10 Data Processors

Cerved Group only resorts to external Data Processors that provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the Data Subject. Any processing performed by a Data Processor is governed by specific contracts that binding on the Data Processor with regard to the Data Controller and that sets out, among other points, the duration, nature and purpose of the processing, the type of personal data and categories of Data Subjects and the obligations and rights of the Data Processor and the Data Controller.

3.1.11 Services provided by Cerved Group in which it acts as Data Processor

To provide certain services, Cerved and/or other Group companies may process personal data on behalf of other Group companies (i.e. provide 'shared services') and/or, more importantly, on behalf of its customers, who as Data Controllers designate Cerved Group as the Data Processor, with the associated obligations and rights.

The processing of personal data by Cerved Group companies as Data Processor – in connection with services such as information gathering, credit assessments and debt collection – are governed by specific Personal Data Processing agreements between Cerved Group companies and/or between the Group and its customers pursuant to article 28 of the GDPR. Such agreements are monitored by the companies, departments and functions that establish and manage contractual relations with the same customers (through respective Privacy Delegates and Privacy Contacts), in order to activate consequent procedures and measures stipulated by the GDPR, including but not limited to: an assessment of compliance with '*privacy by design and by default*' requirements; the inclusion in Cerved Group companies' Data Processing records of their activities as Data Processor; the adoption of sufficient security measures; and the initiation of the DPIA procedure.

3.2 Procedures and regulations adopted to protect personal data

Cerved Group has established a series of internal organisational and technical measures to guarantee – and to be able to demonstrate in accordance with the principle of accountability – that Data Processing is performed in compliance with the provisions of the GDPR. Specifically, these measures include: i) drafting an organisational model that assigns roles and responsibilities, formalises appointments to roles, and establishing traceable processes, procedures and oversight; ii) providing training and informational programmes on personal data protection to employees and individuals who cover specific roles; iii) the creation of supporting documents for related operations such as the *Personal Data Processor Task Handbook*, the *Guidelines on Persons Authorised to*

Process Personal Data, the *Use of IT Tools Policy* and the *Procedure for Handling Personal Data Breaches*.

3.2.1 Information to provide and obtaining consent

Cerved Group undertakes to collect only personal data that is necessary and relevant to the purposes of the respective statutory activities pursued, in accordance with the general principles of lawfulness, fairness and transparency, purpose limitation, data minimisation and accuracy, storage limitation, and data integrity and confidentiality, pursuant to article 5 of the GDPR. To this end, the Group will adopt all organisational and technical measures deemed appropriate to guarantee full compliance with these principles.

At the time personal data is gathered from a Data Subject or is acquired from public or private entities other than the Data Subject (within the limits and terms allowed under the regulations), Cerved Group and its companies, within the scope of their respective responsibilities, undertake to provide Data Subjects appropriate prior disclosures containing clear and specific information about the purposes and methods of processing their personal data, about the related legal basis (consent and/or other presumption of legality, e.g. execution of a contract, fulfilment of legal obligations or pursuit of legitimate interests, as is normally the case for the purpose of gathering business information), about the scope of potential communication to recipients of the data, including subjects that may be established outside the European Union, about the data retention period, about the Data Subject's rights, as well as the information on the Data Controller and the DPO's contact details.

Specifically, in order to comply with the GDPR, Cerved Group:

- has updated disclosure statements and request for consent forms in line with GDPR requirements (such as the Privacy Notice for customers, employees, candidates, suppliers, visitors, etc.);
- gathers the various forms in use and official data protection documentation of the Cerved Group, places them in repositories and makes them available internally in a specific section of the intranet, as well as externally with regard to relevant documents on appropriate pages of the corporate website www.cerved.com;
- establishes methods for updating and managing disclosure and consent forms, for delivering and/or communicating the changes to Data Subjects, as well as for collecting, registering and storing consents and withdrawals of consent, identifying the roles and responsibilities assigned to the various units or functions of Cerved Group companies.

3.2.2 Suppliers and other third parties: contracts with Data Processors

As part of its aim to protect personal data, the GDPR regulates situations in which data is processed by third-party Data Processors on behalf of the Data Controller, specifying the roles and responsibilities for both the Data Controller and the Data Processor. In this respect, in order to comply with the GDPR in such cases, Cerved Group has prepared:

- a standard form contract, entitled the Data Processing Agreement (DPA), which includes specific clauses (e.g. for the transfer of data outside the EU, and on the use of sub-processors) with attachments, so as to regulate relations with external Data Processors and related obligations;
- specific instructions for selecting and managing suppliers, as well as for the signing and archiving of Data Processing contracts;
- an archive of the form contracts to use as well as of those already stipulated.

3.2.3 Records of processing activities

The Data Processing Record ('**Record'**) must contain, pursuant to the GDPR, a minimum set of information, which is different for Data Controllers and Data Processors. The Data Controller's Record must contain: (a) the name and contact details of the data controller and, where applicable, those of the data controller's representative and of the DPO; (b) the purposes of the processing; (c) a description of the categories of Data Subjects and of the categories of personal data; (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation; (f) where possible, the envisaged time limits for erasure of the different categories of data; (g) where possible, a general description of technical and organisational security measures. The Data Processor's Record must contain the information in points (e) and (g) above, plus (h) the name and contact details of the data processor or data processors and of each data controller on behalf of which the data processor is acting, and, where applicable, of the data controller's or the data processor's representative, and the data protection officer, and (j) the categories of processing carried out on behalf of each data controller.

To ensure full compliance with these GDPR rules on records of processing activities (article 30), each Cerved Group company has created an electronic document specifically as its Records of processing activity both as Data Controller and as Data Processor, containing all the required information cited above.

These Records, which the DPO may access for monitoring activities, are made available to the relevant corporate units and can be consulted through specified folders shared between the

Privacy Delegates and Privacy Contacts, for the purpose of viewing updates, entering new processing activities, or in the event of amendments to or termination of existing processing entries, which each unit must carry out or in any case report.

3.2.4 Retention period for personal data

As part of the information to provide the Data Subject, the Data Controller must confirm or determine the retention period for personal data processed, or the criteria used for determining this period, after which personal data is to be rendered anonymous and/or deleted. In order to ensure that it upholds the principle of limited data retention set forth in the GDPR, Cerved Group has therefore established:

- guidelines for criteria to follow when determining the time frame and the terms and conditions for retaining personal data, based on the principles established in data protection regulations and in other applicable legislation with regard to the various business units of each Cerved Group company;
- an operational process that governs the activities of the various offices related to determining, validating and monitoring new data retention periods.

3.2.5 Data protection by design and by default

The Data Controller, from the moment in which Data Processing activity is *designed*, must implement appropriate technical and organisational measures to effectively implement the principles of personal data protection, and must integrate the necessary safeguards into the processing in order to meet the regulatory requirements and protect the rights of Data Subjects, taking into account the state of affairs, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the Data Processing.

The Data Controller must also guarantee that, *by default*, only personal data that is necessary for each specific purpose of the processing are actually processed. This obligation applies to the amount of data collected, the extent of processing, the retention period and accessibility to the data.

To adhere to these principles, all companies, management teams, departments and business units of the Cerved Group must, whenever designing or carrying out new projects, services, systems, etc. that entail processing personal data, ensure that they meet the requirements of data protection both ‘by design’ and ‘by default’; this implies following company methodology that aims to illustrate how Group companies have adopted internal oversight policies, procedures, standard documented practices and security measures to align Personal Data Processing with the new

protection principles. These units must also request specific pertinent safeguards and functions from suppliers, software developers and other third parties during the design phase of such projects, and be able to verify the assessments performed. In particular, wherever a new project, service, system or activity implies processing personal data, the unit engaging in this activity must verify the technical documentation, safeguards, functions and measures adopted by the supplier to ensure personal data minimisation as well as minimisation of the potential risks of processing for the Data Subjects. To assess the adequacy of the supplier as regards data protection, they must therefore work with the IT function and with the DPO, by providing them with all the information and documents needed for this purpose. Wherever such verification brings to light a high risk of failing to guarantee the Data Subject's rights in connection with the new project, service or activity, then the relevant unit must initiate the DPIA procedure as described in section 3.2.8 below. The unit must nevertheless retain all documents collected, including those from suppliers, in relation to the verifications and activities carried out in the interest of compliance with the requirements of data protection by design and by default.

3.2.6 Security of personal data

The Data Controller or Data Processor, taking into account the status, implementation costs, nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Controller and the data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including:

- pseudonymisation 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 procedure for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

For computer systems, Cerved, through its IT structures, undertakes to establish methods to conduct data security risk analysis with respect to the points listed above and, in order to outline appropriate measures to mitigate such risks, also undertakes to verify the suitability and effectiveness of organisational and technical measures adopted and to be adopted for the purpose of ensuring compliance with the provisions of the GDPR, as well as to collect, retain and update all related documentation.

The aim of this risk analysis is to identify any threats that may pose risks to IT systems and/or to the information to be processed, and subsequently to evaluate whether security measures already in place will provide an adequate level of protection against those threats. Analysing risks is not a merely technical activity carried out by IT personnel; instead, all areas of the Cerved Group are involved in analysing the more general aspects of the situation.

The objective of a security policy can never be total elimination of risks, since that would be unachievable. Any information management system, especially a system based on technically advanced tools, will always be exposed to risks that cannot be totally eliminated. The objective must be to provide an adequate level of protection, assessed as a function of the probability that a risk becomes reality and of its consequences, based on the significance of the information to be processed and on the set of existing protection measures.

Cerved therefore undertakes to perform critical analysis of the data security risks and of the existing protection measures, in an effort to pinpoint areas of vulnerability and, consequently, set up or plan further protection measures that need to be implemented as a result of any such vulnerability. Determining what security measures to implement is therefore the outcome of a careful assessment of the effectiveness of security measures already in place at the time of analysis, an assessment conducted in light of current technological and organisational conditions.

This risk analysis must therefore be conducted according to a pre-established schedule. In conjunction with an evaluation of incidents that have actually occurred, this analysis constitutes a critical component in updating general security policies.

Risk analysis pertains to operators' behaviours, to events that cause damage to Data Processing tools and to external events that would affect the overall information processing scenario.

3.2.7 Reporting Personal Data Breaches

In the event of a breach of personal data, the Data Controller must notify the Authority without undue delay, within 72 hours after having become aware of it wherever feasible. This obligation does not apply only if the Data Controller can demonstrate that the Personal Data Breach in question is unlikely to result in a risk to the rights and freedoms of natural persons. The Data Controller must also notify the Data Subject of such a breach without undue delay in the event of a high risk to the rights and freedoms of natural persons. To this end, Cerved Group has adopted a specific procedure for handling and reporting Personal Data Breaches to the Authority and, if needed, to the Data Subject, which includes a register of Personal Data Breaches where related assessments can be documented.

3.2.8 Data protection impact assessment (DPIA)

The GDPR introduces a further obligation to perform a data protection impact assessment (DPIA) for Data Processing activities begun on or after 25 May 2018 that present high risks to the Data Subjects, in cases expressly indicated in article 35 of the Regulation as well as in a list published by the Authority, also retrievable in the European Data Protection Supervisor's Guidelines. An impact assessment must also be performed in the event of changes made, on or after the above date, to any processing activity if such changes (including if due to the use of new or more sophisticated technology) may have a significant impact on the protection of personal data, thereby increasing risks to the rights of Data Subjects.

In order to guarantee compliance with the requirements described above, prior to beginning any new Personal Data Processing activity, the Cerved Group unit that manages the existing activity (the 'process owner') must consult with the IT function and with the DPO, to determine together whether such processing entails "a high risk to the rights and freedoms of natural persons" considering the nature, subject, context and purposes of the processing, especially if the use of new technology is envisaged and/or if it falls within the cases specified in the GDPR and/or in the Authority's list; the assessments carried out must be documented. If it is deemed to be high-risk processing, then the business unit must request initiation of the DPIA procedure expressly outlined by the Cerved Group, beginning consultations with the DPO and with other relevant units (e.g. IT); furthermore, if the DPIA indicates that the processing does entail a high risk despite measures identified to mitigate the risk, then the activity must be submitted for prior consultation with the Authority.

3.2.9 Transfers of personal data to non-EU countries or international organisations

Transfers of personal data to third countries (i.e., those outside the European Union and European Economic Area) may fall under the GDPR only if the country in question guarantees an adequate level of personal data protection. The European Commission has the power to determine the adequacy of a country's protections via a specific decision. With regard to countries not considered adequate, transfers of personal data are prohibited unless legally binding adequate safeguards are agreed between the parties involved.

In the event of a personal data transfer to third countries, each function or unit of Cerved or other Group companies must verify in advance:

- the Commission's decision regarding the adequacy of all third countries in question;
- for all third countries declared not adequate by the Commission, adequate safeguards must be obtained prior to transferring the personal data, including:

- a 'Privacy Shield', in other words, mutual acceptance of the framework agreement that regulates transfers of personal data between the EU and the USA;
- 'binding corporate rules' approved by the authorities as a contractual agreement that enables data transfers between companies within a single group of companies;
- 'standard contract clauses' approved by the European Commission that provide adequate safeguards.

Potential data transfers outside the EU, which are always to be executed in accordance with the conditions described above, are also subject to careful monitoring by Cerved Group, so as to enable constant updates and alignment with other connected compliance aspects such as records of processing activities, privacy notices to Data Subjects and security measures.

3.2.10 Rights of the Data Subject (GDPR articles 15-22)

The Data Subject has the following rights:

- right of access: right to obtain from the Data Controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and certain information such as the purposes of processing and the categories of personal data concerned;
- right to rectification: right to obtain from the Data Controller the rectification of inaccurate personal data concerning him/her; taking into account the purposes of the processing, the Data Subject has the right to have incomplete personal data completed, including by providing a supplementary statement;
- right to erasure ('right to be forgotten'): right to obtain from the Data Controller the erasure of personal data concerning him or her without undue delay and the Data Controller shall have the obligation to erase personal data without undue delay, where certain grounds apply;
- right to restriction of processing: right to restrict the Data Controller's processing of personal data (e.g. to storage purposes only, excluding any other use) as long as certain conditions apply;
- right to data portability: where personal data is processed by automated means, the Data Subject has the right to have the Data Controller: (i) deliver the personal data or subset thereof to him/her "in a structured, commonly used and machine-readable format" and to keep them in view of further use for personal objectives on a personal device or private 'cloud'; or (ii) transmit those data to another Data Controller "without hindrance", where technically feasible;
- right to object: the Data Subject has the right to object at any time, on grounds relating to his/her particular situation, to the processing of personal data concerning him or her which is

based on public interest purposes or purposes of legitimate interests pursued by the Data Controller, including profiling and direct marketing;

- right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, except under certain conditions.

The Data Controller must respond to the Data Subject's request to exercise any of the above rights without undue delay and within one month at the latest (or within a further two months in the event of particularly complex requests, although the obligation to reply within one month still holds).

To comply with the provisions described above, Cerved Group:

- has established a procedure that governs the handling of and responses to requests from Data Subjects to exercise their rights; this procedure identifies the roles and responsibilities assigned to each department or unit of the Group. The aim is to provide practical indications in response to the requests to exercise rights pursuant to articles 15 to 22 of the GDPR and the right to withdraw consent as per article 7.3 of the GDPR. This procedure identifies the data collection sources from which such requests could be received and retraces the actions to be taken in order to provide a timely and accurate response from the Data Controller's, data processor's and joint-controller's point of view;
- dedicated outlets for the submission and collection of requests from Data Subjects;
- a record that tracks requests from Data Subjects of processing managed by Cerved Group, including supporting documentation.

Glossary

Authorised Person	any natural person authorised to access data and/or to process data under the direct authority of the Data Controller or Data Processor (e.g. an employee or contractor of the Data Controller or Data Processor).
Authority	abbreviation used herein for the *Garante per la protezione dei dati personali* (Italian Personal Data Protection Authority).
Data Controller	the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Processing	any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data Processor	a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller (e.g. an IT service provider).
Data Protection Code	Italian Legislative Decree no. 196/2003 of 30 June 2003, entitled the Personal Data Protection Code, as amended by Legislative Decree no. 101/2018, which entered into force on 19 September 2018, providing “Provisions to adjust Italian law to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April

	2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)".
Data Protection Officer (DPO)	the individual (internal or external) appointed by the Data Controller as Data Protection Officer pursuant to article 37 of the GDPR.
Data Subject	a natural person who is identified or identifiable by means of a given set of data.
GDPR or 'the Regulation'	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
Privacy Contact	a natural person appointed by the Data Protection Delegate to cooperate and assist the latter in following and implementing the data protection procedures and guidelines established by the company.
Privacy Delegate	a natural person who, by virtue of and within the limits of his/her designated powers of organisation, management and monitoring, has been delegated by the Data Controller to exercise the functions of managing, coordinating and monitoring Personal Data Processing activities and associated compliance measures required under the GDPR.
Personal Data	any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an

	identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Personal Data Breach	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

APPENDIX I: The Primary Compliance Requirements under the GDPR

Principles of personal data processing

The GDPR essentially confirms (in article 4) the definitions of key terms as already established in the previous legislation (of objects such as 'personal data' and 'processing', and of persons such as the 'data controller' and 'data processor'). Moreover, in article 5 the Regulation confirms the same basic principles applicable to personal data processing, namely that personal data should be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation'); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation'); and (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Information to be provided (Privacy Notice)

Regarding information to be provided when personal data is collected, articles 13 and 14 of the GDPR introduce additional elements beyond those stipulated in the previous regulation, such as requirement to specify the following: the legal basis for the processing; where applicable, to specify the data controller's intention to transfer personal data to a country outside the EU; the time period for which personal data will be stored or the criteria used to determine that period; and that the data subject has the right to lodge a complaint with the relevant supervisory authority. These requirements are in addition to those of providing the identity of the data controller, the purposes of the data processing, the recipients of the personal data, the rights of the data subject including the right to data portability and the right to object to automated decision-making such as profiling. In addition to the content of information, which is to some degree broader than under the legislation previously in force, the GDPR requires the data controller to implement appropriate measures to provide the data subjects with this information and notifications pertaining to exercising their rights in a concise, transparent, intelligible and

easily accessible manner, in clear and plain language, especially where such information is addressed to minors. This information must be provided in writing or by other means including electronic means.

Requirements for lawful processing (consent and other cases)

With regard to lawful processing of personal data, the GDPR essentially confirms in article 6 the same requirement stipulated in the regulations previously in force, namely consent (via an informed positive declaration expressed unambiguously or explicitly, freely, specifically, and this must be adequately recorded), with a series of exceptions to needing consent, such as execution of a contract or pre-contractual measures requested by the data subject, fulfilment of legal obligations, and pursuit of legitimate interests (where consent is required only mainly for marketing purposes, e.g. for sending commercial messages to the data subject via e-mail, fax or text message) and/or for the profiling of customers/users.

In order to process special categories of personal data (formerly known as 'sensitive' data, which includes health-related information, political opinions, trade union membership, etc.) or to process personal data relating to criminal convictions and offences, the GDPR provides (in articles 9 and 10) narrower cases for exceptions to the consent requirement. One main exception is in the processing of employees' personal data in the context of an employment contract, for which the worker's consent is not required as long as it is carried out for the purpose of compliance with legal obligations or collective bargaining obligations. Also, article 9 of the Regulation gives Member States leeway to maintain or introduce further conditions or restrictions regarding the processing of genetic, biometric and health-related data; such conditions will be enumerated as part of the safeguarding measures that the Italian Authority must issue pursuant to article 2-*septies* of the Data Protection Code. For the processing of personal data relating to criminal convictions and offences, article 2-*octies* of the Data Protection Code additionally states that processing is permitted only in cases specifically authorised by a law or regulation; the Code provides an initial list of activities in which such processing is authorised, including anti-money laundering, the defence of legal rights and commercial information; further authorisations are deferred to a regulation yet to be issued by decree by the Ministry of Justice (after consultation with the Authority).

Rights of the Data Subject

The GDPR reinforces the right to erasure (or 'right to be forgotten' – article 17) and also introduces a new right to restricting processing (art. 18) and a right to data portability (art. 20),

while reiterating the other rights already included in the previous regulation, including the right of access, the right to rectification and the right to object.

Persons authorised to process data

The GDPR does not precisely refer to “persons tasked with processing data” as was the case under the Italian Data Protection Code previously in force (the relevant clause was in fact repealed by Legislative Decree no. 101/2018). Instead, the GDPR refers to “persons authorised to process personal data under the direct authority of the data controller or of the data processor”. The data controller or data processor is still required to instruct these persons appropriately regarding the processing (articles 29 and 32, final paragraph); these instructions must be documented, in light of the new principle of accountability, as described in Appendix II below. This principle has been delineated further in article 2-*quaterdecies* of the Data Protection Code, where it is stated that the data controller or data processor may, without ceding their own liability and within their own organisation, assign specific personal data processing tasks and functions to designated natural persons who operate under their authority; the same article states that the most suitable methods of authorising specific persons for personal data processing should be determined.

APPENDIX II: New Compliance Requirements Introduced by the GDPR

The GDPR introduces a significant change to planning and managing compliance with data protection regulations. A system of personal data 'governance' is now needed, as a result of enhanced data controller and data processor accountability as stipulated in article 5: the data controller and data processor must guarantee and be able to demonstrate their compliance with the GDPR provisions. This new framework implies that the data controller has an obligation to implement technical and organisational measures, whose adequacy must be assessed based on specific personal data processing characteristics (the nature, scope of application, context and purposes of processing), as well as on the risks to the rights and freedoms of natural persons (as per article 24). All of the main new aspects introduced under the GDPR are in effect linked to this new framework for planning and managing compliance.

Data Protection Officer (DPO) (articles 37-39)

The DPO role is one of the major new aspects of the GDPR, constituting one of the key elements in data protection compliance. It is mandatory for all public bodies to designate a DPO, while private sector organisations are required to do so only in certain cases described in article 37.

The DPO is a person who must first of all be assigned this role as a function of his/her specialised knowledge of personal data protection regulations and practices, professional qualities and ability to carry out all tasks required. The DPO must also hold an autonomous, independent position in the organisation. In the Cerved Group, the DPO reports directly to the governing body of each Group company.

The DPO's main tasks are to inform and provide advice on applicable data protection regulations to the corporate governing bodies and to Cerved Group employees who execute data processing activities, as well as to oversee observance of the GDPR and of Cerved Group's own personal data protection policies, including the allocation of responsibilities, accountability and training for personnel who perform processing activities and/or related audit activities. In addition, the DPO cooperates and liaises with the Authority on personal data processing matters and may conduct consultations on other matters as needed. The DPO also acts as the contact person for data subjects on all matters concerning personal data processing and their associated rights. The DPO must provide opinions and carry out other tasks based on company procedures in force in terms of determining personal data retention periods, evaluating and reporting data breaches, and conducting DPIAs. The DPO's contact

details must be gathered, made public (for data subjects and employees) and communicated to the Authority.

Records of processing activities (Art. 30)

The GDPR introduces an obligation to maintain records for both the data controller (for processing activities under its responsibility) and the data processor (for processing activities performed on behalf of a data controller).

Data protection by design and by default (Art. 25)

The GDPR establishes that at the time a new processing activity begins or an existing one changes, the data controller must implement measures to abide by data protection principles (protection 'by design'). The data controller must also implement appropriate technical and organisational measures to ensure that 'by default' only personal data that is necessary for each specific purpose of the processing will actually be processed.

Data Protection Impact Assessment - DPIA (Art. 35)

The GDPR establishes that whenever a processing operation is likely to result in a high risk to the rights and freedoms of natural persons, the data controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations.

Notification of a personal data breach (Art. 33-34)

The GDPR introduces an obligation to notify the Authority without undue delay (within 72 hours where possible) of any breaches of personal data; the data subjects in question must also be notified of the breach without undue delay whenever there is a high risk to the rights and freedoms of natural persons.

Data Processor (Art. 28 and 82)

The GDPR sets out specific obligations and duties for data processors. The data processor may engage another person ('sub-processor') to help carry out the processing, providing authorisation to do so is granted by the data controller, where the sub-processor (through a contract or other appropriate legal act) takes on the same obligations as the data processor with respect to the data controller.

Security of processing (Art. 32)

The importance of security obligations, established in previous regulations, is confirmed by the GDPR, but there are no longer 'minimum' security measures, as both the data controller and the data processor are required to implement technical and organisational measures to ensure a level of security that is appropriate to the risks involved.

Certification of data processing (Art. 42-43)

The GDPR introduces an option to seek data protection certification (or seals or marks) that denote compliance with the GDPR.

Administrative fines (Art. 83)

The GDPR does not stipulate any penal sanctions, leaving member state legislators the freedom to maintain previous ones or introduce new ones. However, it does substantially increase the maximum administrative fines, giving the Authority the option to issue a fine of up to €10 million or, for businesses, of 2% of global annual revenue up to €20 million; for repeat corporate offenders, the fine can rise to as much as 4% of global annual revenue.

Following the revision of the Italian Data Protection Code, some penal sanctions for the most severe illicit conduct (those committed with malicious intent, to exploit or cause harm to the data subject) have been maintained and even increased. Specific crimes include: unlawful processing of personal data relating to special categories of personal data or to criminal convictions or offences (as well as telephone or computer usage data, localisation data and undesired communication – see art. 167 of the Data Protection Code); unlawful communication or dissemination of personal data on a large scale (art. 167-bis; fraudulent acquisition of personal data on a large scale (art. 167-ter); issuing false statements to the Authority and/or hindering the execution of tasks or the exercise of the Authority's powers of supervision (art. 168); and failure to comply with Authority orders (art. 170). Penal sanctions for violations of the regulations regarding remote audits or inspections and regarding worker opinion surveys have remained the same (articles 4, 8 and 38 of Law 300/1970, the Workers' Statute).