



BROADRIDGE FINANCIAL SOLUTIONS, INC.
Global Privacy Policy

Global Privacy Policy

This Global Privacy Policy (this “**Policy**”) specifies policy objectives for the collection, use, maintenance, security and disclosure of Personal Information by Broadridge Financial Solutions, Inc. and its Affiliates (collectively, “**Broadridge**”). This Global Privacy Policy and its related policies and procedures together constitute an integral part of Broadridge’s “**Global Privacy Program**”, which is intended to drive a consistent approach to privacy protection across Broadridge, and provide the basis for an effective Global Privacy Program. Definitions used in this Policy and other documents that are part of the Global Privacy Program are set forth in the Privacy Policy Definitions, attached hereto as Appendix A.

Scope

Business Scope: This Policy applies to Broadridge and all Broadridge Workers.

Subject Matter Scope: This Policy sets forth certain principles that apply to all Processing of Personal Information by Broadridge globally. It is supplemented from time to time by related policies and procedures that state additional requirements for collecting Personal Information or Processing certain specific types of Personal Information, such as information:

- relating to Workers (See Global Human Resources Privacy Policy and its supplements);
- collected pursuant to client contracts (See Client Information Privacy Policy); and
- collected as a result of Broadridge’s marketing activities.

Applicable Regulatory Requirements and Local Laws: Where international, federal, state or local laws or regulations contain stricter requirements, Broadridge’s policy is to Process Personal Information in compliance with such stricter requirements. This Policy may be supplemented by other policies and procedures as required by, or appropriate in light of, such laws or regulations.

Policy Statement

All Processing of Personal Information of any type by Broadridge or on its behalf is to be handled in accordance with the privacy principles set forth in this Policy, and as required by applicable law or regulation. These principles apply regardless of whether Broadridge creates or generates Personal Information, or whether Personal Information is provided to Broadridge by Clients, Workers, job candidates or other third parties, and whether Broadridge is acting as a Data Processor or Controller. Specific requirements relating to Broadridge acting as a Data Processor or Controller can be found in related policies and procedures within the Broadridge Global Privacy Program.

Data Privacy Principles

The use of Personal Information by Broadridge, by Workers or service providers on its behalf must comply with the following principles:

Fairness, lawfulness and transparency. Personal Information is to be Processed fairly, lawfully, and in a transparent manner, and with the knowledge of the party providing such Personal Information, whether an individual or Client (except where applicable law provides otherwise). Broadridge will Process

Personal Information when it has a legal basis for doing so. Where applicable law requires, Broadridge will obtain individuals' prior consent to use their Personal Information. Broadridge strives to provide clear and easily accessible notices to individuals from whom Personal Information is collected directly, to inform them about how their Personal Information is handled. If Broadridge collects or receives Personal Information in its capacity as a service provider or Data Processor for Clients, the Clients will be responsible for determining the legal basis, providing notice and obtaining consent, and Broadridge will assist in providing notice and obtaining consent where requested.

Purpose limitation. Personal Information should only be collected for legitimate Business Purposes, as specified and made explicit in the notice provided to individuals or in a written contract with a Client. Personal Information should not be further disclosed, made available or otherwise used in a manner that is incompatible with those Business Purposes, except as specifically provided or required by applicable law. Whenever Personal Information is to be Transferred to or shared with a third party, whether or not a Broadridge Affiliate, reasonable steps should be taken to ensure that the receiving entity will handle the Personal Information within these limitations.

Data minimization and storage limitation. Broadridge seeks to limit the collection and use of Personal Information to what is necessary to achieve its legitimate, specified and explicit Business Purposes. Personal Information that Broadridge collects or uses should always be sufficient for and relevant to those Business Purposes, and obtained by lawful and fair means. Personal Information should be retained in a form that permits identification of individuals for no longer than is necessary to achieve the specified, explicit and legitimate Business Purposes for which it is collected.

Security, integrity and confidentiality. Broadridge aims to employ at all times administrative, technical and physical safeguards that are reasonably designed to maintain the confidentiality of Personal Information and protect, proportional to the sensitivity of the Personal Information being protected, Personal Information against loss and the unauthorized or unlawful access, use, modification, disclosure, damage or destruction of Personal Information, in accordance with applicable laws and regulations.

Individuals' choice and rights. Broadridge recognizes, in accordance with applicable law, individuals' rights with respect to their Personal Information, such as rights: (a) to obtain confirmation of whether or not Broadridge has Personal Information relating to an individual; (b) to receive a copy of its Personal Information; and (c) to have their Personal Information corrected, completed, amended or destroyed. Wherever appropriate under applicable law, Broadridge will allow individuals who provided Personal Information directly to Broadridge to exercise choice in relation to the collection, use, disclosure and destruction of their Personal Information. If Broadridge collects or receives such Personal Information in its capacity as a service provider for Clients, Broadridge will assist Clients as needed to help them respond to such exercises of choice.

Adequate assistance. Broadridge aims to make readily available to Workers adequate assistance in establishing the existence and nature of Personal Information it collects or uses in any way, and the main purposes of its use.

Accountability. Broadridge will strive to be accountable for, and demonstrate compliance with, its policies, procedures and measures designed to give effect to the principles set out in this Global Privacy Policy, as well as requirements of applicable laws and regulations.

Violations

Broadridge takes all allegations that this Policy has been violated seriously. Any Worker who receives a privacy complaint or becomes aware of a possible violation of this Policy should immediately report the complaint or concern to the local Privacy Officer, the Chief Privacy Officer, the Business Information Security Officer (“**BISO**”), his/her supervisor, human resources department manager or a member of the Legal Department. Broadridge will also carefully consider all allegations that Personal Information has not been protected appropriately, even if such allegations fall outside of scope of this Policy.

All Workers must immediately report any actual or suspected security incident related to Personal Information to the Broadridge Incident Response Team (See “**For More Information/Reporting**”). Broadridge investigates these incidents and takes those steps necessary to mitigate possible harm and comply with applicable laws.

Broadridge will work closely with its Clients regarding any allegation that this Policy has been violated regarding Client Personal Information or in the event of any security incident involving Client Personal Information.

Privacy Program Governance

The Global Privacy Program is intended to support compliance with this Policy and related policies and procedures, and with applicable laws or contractual agreements governing the handling of Personal Information. Broadridge has designated a Chief Privacy Officer, and appropriate privacy leaders who are responsible for overseeing implementation of the Global Privacy Program (“**Privacy Officers**”). The Chief Privacy Officer communicates Global Privacy Program expectations to these privacy officers and assists them as they implement the program locally. Please see Broadridge’s Privacy Governance Policy for more information on the individuals who support the Global Privacy Program.

Related Policies and Procedures

The Broadridge Global Privacy Program consists of this Global Privacy Policy and related privacy policies and procedures, including:

Privacy Policy Definitions

Privacy Governance Policy

Client Information Privacy Policy

Global Human Resources Privacy Policy

- North America Human Resources Privacy Supplement
- European Economic Area/United Kingdom Human Resources Privacy Supplement
- AsiaPac and Russia Human Resources Privacy Supplement

All Broadridge privacy policies constituting the Global Privacy Program and a list of the Privacy Officers can be found on [**MyBroadridge**](#).

More Information related to Broadridge’s Global Privacy Program can also be found in Broadridge’s Information Security Policy and its related policies, methodologies and standards.

For More Information/Reporting

For more information regarding the Global Privacy Program, please contact your local Privacy Officer or BISO, the Chief Privacy Officer, the Legal Department, Human Resources or the Information Security Group. To report a suspected or actual security incident, please initiate such report on MyBroadridge at [Report an Incident or Concern](#), by contacting your local Privacy Officer or a member of the Broadridge Information Security Group at 631-254-7500 or SIRT@Broadridge.com.

APPENDIX A

Privacy Policy Definitions

Affiliate – Any company that is directly or indirectly wholly-owned by Broadridge.

Business Purposes - Means the following purposes for which Personal Information may be generally Processed:

- To provide the information, product, service or solution requested or contracted for by a Client or individual, or as reasonably expected given the context in which the Personal Information was collected (such as providing services ancillary to the information, product, service or solution requested or contracted for, including account management);
- For managing Broadridge’s Workers and their employment by Broadridge;
- For identity and credential management, including identity verification and authentication, and technology administration;
- To protect the security and integrity of Broadridge’s systems, networks, applications and data, including detecting, analyzing and resolving security threats, and collaborating with cybersecurity centers, consortia and law enforcement about imminent threats;
- For legal and regulatory compliance, including all uses and disclosures of Personal Information that are required by law or as reasonably needed for compliance with Broadridge’s programs, policies and procedures, such as anti-money laundering programs, security and incident response programs, intellectual property protection programs, and corporate ethics and compliance policies;
- For corporate audit, analysis and reporting, to enforce Broadridge contracts, to protect against injury, theft, legal liability, fraud or abuse, to protect people or property, including fraud prevention programs and physical security programs (subject to applicable laws);
- To make back-up copies for business continuity and disaster recovery purposes;
- For analytics, benchmarking, industry reporting and product development (e.g., de-identification of Personal Information to derive anonymized or aggregated datasets); and
- For corporate reorganization, including mergers, acquisitions and divestitures.

Client – An entity that engages Broadridge to provide information, products, services or solutions, which may include Processing of Personal Information on its behalf. In particular, Clients engage Broadridge to provide various data processing services, which often are part of our investor communication solutions and securities processing and operations solutions that require collecting, analyzing and Processing data, including Personal Information about Client’s customers and other individuals.

Controller – With respect to any Personal Information, the entity that determines the means and purposes of Processing. For example, Broadridge is the Controller with respect to its own human resources Worker data and business data (such as data collected as part of marketing activities or Client billing information), while each Broadridge Client is the Controller for Personal Information Processed by Broadridge to provide information, products, services or solutions for the Client.

Data Processor – With respect to any Personal Information, an entity that Processes the information at the request of and pursuant to instructions from the Controller. For example, Broadridge is a Data Processor with respect to the information it handles when performing services for Clients.

Personal Information – Any information that relates to an identified or identifiable individual. “Identifiable” means that data, whether alone or when used in combination with other information, can be used to identify, locate, contact or target an individual. Personal Information can be in any media or format, including computerized or electronic records as well as paper-based files. There may be slight differences in the definition of Personal Information from country to country.

Processing – Any operation or set of operations performed upon Personal Information, whether or not by automatic means, such as collection, accessing, anonymizing, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, Transfer, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking or dispersed erasure or destruction, and “Process” and “Processes” will be understood accordingly.

Sensitive Personal Information – Sensitive Personal Information is a subset of Personal Information, which due to its nature has been classified by law or by policy as deserving additional privacy and security protections. Sensitive Personal Information includes, but may not be limited to, the following:

- All government-issued identification numbers (including U.S. Social Security numbers, Canadian Social Insurance numbers, other national identification numbers, driver’s license numbers and passport numbers);
- Individual financial account numbers (bank or broker account numbers, credit card numbers and other information), account log-in, password, or credentials allowing access to an account and related financial account information;
- Individual medical records, health and disability information, genetic information and biometric information, including all information that is regulated as “Protected Health Information” under the United States Health Information Portability and Accountability Act (“HIPAA”), individual health or insurance account access credentials, such as user names, passwords and security questions;
- Consumer reporting data, including employment background screening reports, as subject to the United States Fair Credit Reporting Act and similar legislation in other countries;
- An individual’s precise geolocation; and
- The contents of an individual’s consumer’s mail, email, and text messages unless the business is the intended recipient of the communication.

Special Categories of Personal Information - namely, data elements revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual orientation or sex life, medical or health conditions, and criminal convictions and offenses, including those of a partner or spouse or family in certain instances.

Standard Contractual Clauses – The form contracts promulgated by the European Commission to provide safeguards for Personal Information Transferred from the European Economic Area, and Switzerland as well as the form contracts promulgated by the Information Commissioner’s Office of the United Kingdom under S119A(1) Data Protection Act 2018.

Information about these model contracts can be found online at:

<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN>

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/>

Transfer – Either: (i) the physical movement of Personal Information to a recipient; or (ii) the disclosure of Personal Information to a recipient via remote access. An **International Transfer** is any Transfer of Personal Information to (or disclosure of Personal Information to) a recipient located in a different country.

Workers – All employees, on-site contractors and other individuals who are engaged by Broadridge and who have access to a Broadridge facility, systems or data.