Global Privacy Policy

Updated as of August 24, 2020

This Global Privacy Policy (the "Policy") specifies the requirements for the collection, use, maintenance, security and disclosure of Personal Information by Broadridge Financial Solutions, Inc. and its Affiliates (collectively, "Broadridge").

Scope

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

Subject Matter Scope: This Policy applies to all "Processing" of "Personal Information" by Broadridge globally. It may be supplemented by other policies and procedures that state additional requirements for collecting Personal Information or Processing certain specific types of Personal Information, such as Personal Information relating to employees, or for Processing Personal Information in certain geographic regions.

Applicable Regulatory Requirements and Local Laws: Where national, state or local law or regulations contain stricter requirements, Broadridge will only Process Personal Information in compliance with such stricter requirements. This Policy may be supplemented by other policies and procedures as needed to demonstrate compliance with these laws.

A complete list of supplemental policies and implementing procedures is included in Annex 1.

Definitions

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

Business Contact Information – Business contact information ("BCI") consists of those data elements that are commonly found on business cards, such as: name, title, company name, mailing email address and telephone numbers.

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 data and business information, while each Broadridge Client is the Controller for Personal Information Processed by Broadridge to perform services for the Client.

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

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

EEA Personal Data – A subset of Personal Information that consists of Personal Information about individuals who reside in the European Economic Area,[1] Switzerland and the United Kingdom.

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

- To provide the information, product or service requested by the individual or as reasonably expected given the context in which with the Personal Information was collected (such as providing customer service);

- For identity and credential management, including identity verification and authentication, and technology administration;

- To protect the security and integrity of 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 company policies and procedures, such as: anti-money laundering programs, security and incident response programs, intellectual property protection programs, and corporate ethics and compliance hotlines;

- For corporate audit, analysis and reporting, to enforce our contracts and 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; and

- For corporate governance, including mergers, acquisitions and divestitures.

Personal Information – Any information that (alone or when used in combination with other information within Broadridge's direct control) can be used to identify, locate, contact or target an individual. Personal Information includes, for example, names, email addresses, financial account numbers, government-issued identification numbers and other user identification numbers (such as GUIDs), as well as other information relating to the individual that is associated with the Personal Information. Personal Information can be in any media or format, including computerized or electronic records as well as paper-based files.

Processing – Any operation or set of operations performed upon Personal Information, whether or not by automatic means, such as collection, 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.

Professional – An individual (other than a Worker) who interacts with Broadridge in a business,

[1] The European Economic Area consists of the EU member states (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden) plus Norway, Lichtenstein and Iceland. *Switzerland and the UK are not part of the EEA, but these countries' privacy laws are similar to those found in the EEA countries, so we treat Swiss and UK residents as if they were in the EEA for purposes of this Policy*.

commercial or professional capacity. For example, this would include commercial customers, vendors, collaborators, and business partners.

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 US Social Security numbers, Canadian Social Insurance numbers, other national identification numbers, driver's license numbers, and passport numbers);
- Individual financial account numbers (bank account numbers, credit card numbers, other information if that information would permit access to an individual's financial account) and 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 account access credentials, such as usernames, 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;
- Data related to criminal convictions or offenses or allegations of crimes; and
- "Special Categories of Data" namely, data elements revealing race, ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or sex life.

Standard Contractual Clauses – The form contracts promulgated by the European Commission which assures adequate protection for Personal Information transferred from Europe. Information about these model contracts can be found online at: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

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. A ***Cross-Border 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 have independent access to a Broadridge facility, systems or data.

Policy Statements

1. Policy Statements for Broadridge as a Controller

1.1 Collection and Use of Personal Information

Broadridge collects and uses Personal Information for its own business purposes in a reasonable and lawful manner. In general, we use Personal Information to:

- Develop relationships with current and prospective Clients and Workers*;*
- Provide services to our Clients and their customers;

- Ensure the security and integrity of financial transactions;
- Operate our business, such as for human resources, information technology and other company functions; and
- Comply with legal and regulatory requirements.

We may also use Personal Information:

- For the purposes listed in the applicable privacy notice;
- For the purposes for which the individual would reasonably expect the information to be processed (such as responding to an inquiry) and similar closely related purpose;
- If we have the individuals' consent;
- For our Everyday Business Purposes; and
- As otherwise permitted by law.

For a complete list of approved business purposes, see Annex 2.

1.2 Privacy Notices – Transparency

Broadridge will provide individuals whose Personal Information is collected by Broadridge with a privacy notice that generally states:

- the types of Personal Information collected and the sources from which the Personal Information is collected (if not from the individual directly);
- the purposes and uses for which the Personal Information will be Processed;
- the types of recipients to whom the Personal Information may be disclosed;
- that the Personal Information may be transferred to third countries;
- that reasonable privacy and security safeguards are employed; and
- the rights and choices that the individuals may have with respect to their Personal Information.

At a minimum, an appropriate privacy notice will be provided at each data collection point (such as on Broadridge websites and mobile apps) and provided upon request. Local laws may have additional requirements that must be met regarding privacy notice content, format, language or delivery, and our notices will be tailored to address these rules.

1.3 Consent and Accommodation

Broadridge will provide individuals with a reasonable opportunity to object to the Processing of their Personal Information. Where possible, Broadridge will seek to make reasonable accommodations when an individual has concerns regarding the Processing of his or her Personal Information.

- Where local laws require the express or explicit consent of the individuals for the collection and other Processing of their Personal Information, Broadridge will obtain such consent.
- Where reasonably possible, individuals must be allowed to revoke their consent after they have

provided it. However, under certain circumstances, such as in connection with employment, revocation of consent will be limited and may result in loss of privileges or rights for the individual.

- Consent and accommodation are not generally required for the Processing of Personal Information (including Sensitive Personal Information) where local laws impose obligations on Broadridge to process Personal Information.

1.4 Internal and External Disclosures; International Data Transfers

(a) ***Internal Disclosures.*** Taking into account the sensitivity of Personal Information, Broadridge will limit disclosures of Personal Information within the company and across its Affiliates to those Workers who reasonably need access to such Personal Information to carry out their assigned functions in an efficient and effective manner. For example, Broadridge may provide Workers with broad access to Business Contact Information but highly restricted access to Sensitive Personal Information

(b) ***External Disclosures.*** Taking into account the sensitivity of the Personal Information, Broadridge will Transfer Personal Information to third parties only when (i) such third parties are acting on Broadridge's behalf or in furtherance of its business and such third parties are bound by law or contract to limit their own use of the Personal Information for appropriate purposes, consistent with the Collection and Use section above, (iii) the disclosure is otherwise legally permitted, (iv) with the consent of the individual, or (v) in the event of an emergency.

- Broadridge will only disclose to third parties those elements of Personal Information that are reasonably necessary to meet the business needs of Broadridge or to comply with a legal requirement.

- Broadridge will only disclose Sensitive Personal Information to third party processors or business advisors who are legally or contractually obligated to:
  i. comply with all applicable privacy laws and regulations,
  ii. limit use of the Personal Information to defined, appropriate purposes,
  iii. secure the Personal Information and notify Broadridge of any breaches, and
  iv. undergo periodic assessments by Broadridge or other appropriate third parties.

  Local law, policies and procedures may have additional requirements that must be met with regard to the qualification and use by third party data processors

- All Transfers of Sensitive Personal Information to and from Broadridge must be completed in a reasonably secure manner consistent with the requirements of applicable laws and internal procedures.

(c) ***Business-Necessary Disclosures.*** Broadridge may disclose Personal Information (including Sensitive Personal Information) where needed to (i) affect a license, sale or transfer of business assets, including the license, sale or transfer of rights to a business unit or service or product line, (ii) enforce Broadridge's rights, protect its property, or protect the rights, property or safety of others, or (iii) support external auditing, compliance and corporate governance functions.

(d) ***Disclosures to Government Agencies.*** Broadridge may disclose Personal Information (including Sensitive Personal Information) as required by law. For example, Broadridge is required to disclose Personal Information to taxing agencies about Worker and Professional compensation. Broadridge may also be required to provide Personal Information to government agencies in connection with product and workplace safety reporting. In addition, Broadridge may be required to disclose Personal Information to third parties in connection with legal or regulatory proceedings, such as in response to subpoenas.

(e) ***International Transfers of Personal Information.*** Broadridge may Transfer Personal Information across national borders, but it will comply with those laws that regulate Cross-Border Transfers.

- We obtain consent for Cross-Border Transfers where required by law.

- We use Standard Contractual Clauses to assure adequate protection for EEA Personal Data Transferred to the United States and other countries from the European Economic Area (EEA), the United Kingdom and Switzerland. We may also Transfer EEA Personal Data as authorized by our supervisory authorities or as otherwise permitted by law.

1.5 Access and Correction

Broadridge is committed to providing individuals with a reasonable opportunity to examine their own Personal Information. Where individuals have rights of access, they may also confirm the accuracy and completeness of their Personal Information and have their Personal Information amended, if appropriate.

- The ability to access and correct Personal Information will not be limited by transfers of Personal Information – the ability exists regardless of where Personal Information is physically situated.

- The right of individuals to access their Personal Information is not unlimited, however. For example, access and/or correction may be denied where (i) the costs of providing access are unreasonable given the possible benefit to the individual, or (ii) providing such access or correction could compromise the privacy of another person or unreasonably expose sensitive company information. Additionally, Professionals' rights of access to information may be limited to that Personal Information which is required by law to be accessible.

Details regarding the extent to which access will be provided will be addressed in applicable local procedures.

1.6 Accuracy and Retention

Broadridge will use reasonable measures to keep Personal Information appropriately accurate, complete and up to date, as needed for the Processing being performed. In many cases, Broadridge will rely on individuals to use their ability to access and correct Personal Information to assist with this process.

Personal Information will be retained and destroyed in a manner consistent with applicable information security and document retention policies of Broadridge.

2. Policy Statements for Broadridge as a Data Processor

Broadridge serves as a Data Processor for its Clients when it Processes Personal Information pertaining to its Clients' customers, shareholders and account holders. When serving as a Data Processor:

- Broadridge will only Process Client Personal Information in accordance with its Client contracts and the other instructions that it has received from its Clients**.**

- Broadridge will protect Client Personal Information using information security controls that are at least as stringent as Broadridge uses to protect its own Personal Information.

- Broadridge understands that Client Personal Information is subject to U.S. federal, U.S. state and international data protection laws, including (without limitation) the Gramm-Leach-Bliley Act, HIPAA, EU General Data Protection Regulation and other regulations requiring specific security controls and security breach notification. Broadridge will comply with all laws applicable to it as a Data Processor for Client Personal Information.

- Broadridge may disclose Client Personal Information to Affiliates and third-party processors as needed to perform the services requested by the Client. Broadridge will require all Affiliates and third party processors to comply with appropriate privacy and security requirements.

- Broadridge may disclose Client Personal Information as required by law. Unless prohibited from doing so, Broadridge will inform its Client prior to making any such required disclosures and will reasonably allow the Client to take steps necessary to protect the Personal Information.

- Broadridge relies on its Clients to manage compliance with all aspects of data protection law applicable to them as Data Controllers. For example, Broadridge's Clients are responsible for confirming that the Processing requested meets applicable legal requirements, providing its their customers, shareholders and account holders with required privacy notices, and respecting their privacy rights. Broadridge will use reasonable efforts to assist Clients as needed with privacy compliance. For example, Broadridge applications that collect Personal Information will include notices referring individuals to the Client for privacy questions.

- Broadridge will use reasonable efforts to be transparent with Clients about its Processing activities. Broadridge will work with Clients as needed to authorize Cross-Border Transfers of Client Personal Information. Broadridge is committed to handling Client Personal Information in accordance with applicable laws. Client Personal Information may be Transferred to, stored at or Processed in the United States and other countries which may not have equivalent privacy or data protection laws. Regardless of where Client Personal Information is transferred, Broadridge will protect such Client Personal Information in accordance with this Policy.

- If Broadridge becomes aware of any actual or suspected misuse of Client Personal Information or unauthorized access that compromises the security, integrity or confidentiality of any Client Personal Information, Broadridge will take appropriate actions to contain and mitigate the incident, including promptly notifying the Client.

- All external Broadridge websites and mobile applications that are used to collect Personal Information for Clients will link to either the Client's own privacy statement or to Broadridge's Global Privacy Statement. Broadridge's Global Privacy Statement describe the practices that Broadridge will follow with respect to the personal information it collects from users of hosted websites and applications.

3. Security and Incident Response

Broadridge employs administrative, technical and physical safeguards that are reasonably designed to maintain the confidentiality of Personal Information and protect Personal Information from (i) anticipated threats or hazards, and (ii) unauthorized access or use. In each case, Broadridge will strive to provide security that is proportional to the sensitivity of the Personal Information being protected, with the greatest effort being focused on protecting Sensitive Personal Information.

Broadridge maintains a formal Incident Response Program to allow it to respond effectively to security incidents that involve Personal Information. All Workers must immediately report any actual or suspected security incident to the Broadridge Incident Response Team. Broadridge investigates these incidents and take those steps necessary to mitigate possible harm and comply with applicable laws.

4. Privacy Program Governance

Broadridge maintains a privacy program to support compliance with this Policy and any applicable laws or contractual agreements governing the handling of Personal Information.

- Broadridge has designated appropriate privacy leaders ("privacy officers") who are responsible for overseeing implementation of the privacy program. The Chief Privacy Officer communicates global privacy program expectations to these privacy leaders and assists them as they implement the privacy program locally.

- Taking into account the sensitivity of the Personal Information, all Workers who access Personal Information are trained as is appropriate for their Processing of Personal Information.

- All Affiliates are obligated to ensure that their implementation of this Policy complies with applicable local laws. This Policy may be supplemented with an Affiliate policy for those Affiliates where local laws impose greater obligations.

- The Chief Privacy Officer publishes procedures and guidelines to help ensure consistent implementation of this Policy across Affiliates. ***See Annex 1.*** Given the global nature of this Policy and variations in local law and custom, it is also anticipated that Affiliates will have local procedures that will vary in their approach to implementation of this Policy. In some cases, local laws may impose different requirements on an Affiliate.

- The Chief Privacy Officer, the privacy officers and their respective designees maintain records as needed to demonstrate compliance with this Policy and applicable laws.

- For more information regarding Broadridge's privacy program, please see the contact information specified below in the section titled "For More Information."

5. Violations

Broadridge takes all allegations that this Policy has been violated seriously. 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.

- 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), to his/her supervisor, human resources department manager or a member of the Legal Department. The Chief Privacy Officer or the BISO will trigger the company incident response plan if applicable.

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

6. For More Information

For more information regarding this Policy or the Broadridge Privacy Program, please contact the individuals set forth below, the Legal Department, Human Resources, the Information Security Group or your local BISO. In addition, there is an information security incident reporting procedure that can be initiated on Broadridge Central at Incident Reporting or by any of the privacy officers or by a member of the Broadridge Information Security Department.