

Name: Safe Harbor Privacy Policy for Employees	Policy Number: P.01.01
Department Name: Brunswick Legal Department	Page: 1 of 6
Original Issue Date: April 22, 2013	Revision Date: N/A
Policy Owner: Brunswick Privacy Office	Policy Contact Person: General Counsel

Purpose and Applicability

This Brunswick Safe Harbor Privacy Policy for Employees (“Policy”) explains how Brunswick Corporation and its affiliates (“Brunswick”) collect and process Personal Data relating to full-time and part-time temporary and/or regular personnel, job applicants, consultants or contractors in the United States, European Economic Area (“EEA”) and Switzerland. The Policy applies to Personal Data of such individuals in any electronic format or collected via electronic means.

Any individual or entity who, on Brunswick’s behalf, collects and/or processes electronic Personal Data related to Data Subjects in the U.S., EEA or Switzerland must comply with this Policy.

Definitions

Agent: Any individual or entity that processes Personal Data under Brunswick’s direction, including, but not limited to, payroll providers, software developers or providers, benefits brokers, benefits providers, training providers, human resources consultants, insurance companies and tax and accounting firms.

Data Subjects: Employees, job applicants, consultants and contractors.

Data Collection Points: Online, telephone, fax, e-mail, or other electronic means from which Personal Data is collected. Human Resources Data Collection Points may include online forms and questionnaires, resumes and job applications; electronic records of interviews/meetings with Data Subjects and/or discussions with supervisors and peers; and employment contracts in electronic form.

Employees: Temporary and regular personnel, whether full-time or part-time.

European Economic Area (EEA): Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, the United Kingdom (including England, Scotland, Northern Ireland and Wales) and any other countries which may later be deemed part of the EEA.

Onward Transfer: A transfer of Personal Data to Agents or Third Parties, including making such data available to Agents or Third Parties.

Personal Data: Electronic data about an identified or identifiable individual, received, obtained or held by Brunswick. Personal Data includes (but is not limited to): name, date of birth, passport number, home contact information, business contact information, marital status, family members’

information, emergency contact information, qualifications and employment history, employment terms and conditions, employment status, working hours, hire category, salary, employee benefit plans, attendance records, performance reviews, reporting structure, background check information (where permissible by law), tax reporting information, disciplinary and grievance communication, photographs and information related to Brunswick-issued equipment including phones, vehicles, credit cards, and similar information.

Processing: Any operation or set of operations performed upon Personal Data, whether or not by automatic means. It includes collecting, retaining, recording, organizing, storing, adapting or altering, retrieving, consulting, using, disclosing, disseminating or otherwise making available, blocking, erasing or destroying Personal Data. Processing also includes activities such as copying, filing and inputting Personal Data into a database.

Safe Harbor: The United States (U.S.) Department of Commerce (“DoC”) and the European Commission, and the DoC and the Federal Data Protection and Information Commissioner of Switzerland, have separately agreed on data protection principles (collectively, the “Safe Harbor Principles”) to enable U.S. companies to transfer Personal Data from the EEA and Switzerland to the U.S. in a manner that complies with European and Swiss law. Participation in the Safe Harbor allows Brunswick to legally transfer Personal Data from the EEA and Switzerland to the United States.

Sensitive Personal Data: Electronic personal data that relates to a Data Subject’s medical or health condition(s), race, national origin, political opinions or affiliations, religious or philosophical beliefs, trade union membership or sex life information.

Third Party: An individual or entity not an Agent, not affiliated with Brunswick and that does not act on Brunswick’s behalf or under Brunswick’s direction.

Safe Harbor

Consistent with its commitment to protect privacy, Brunswick complies with the U.S.-EU and U.S.-Swiss Safe Harbor Framework and adheres to both sets of Safe Harbor Principles. For more information about the Safe Harbor Principles, please visit the U.S. Department of Commerce’s Website at <http://export.gov/safeharbor/>.

Policy Guidelines

- A. Company Security. Pursuant to this Policy and Brunswick’s data security procedures, all individuals to whom this Policy applies must comply with Brunswick’s administrative, technical and physical safeguards to protect Personal Data from loss, misuse, unauthorized access, disclosure, alteration and destruction.
- B. Agent Security. Brunswick may authorize the transfer of Personal Data to an Agent under one of the following conditions:

- i. the Agent is certified under the applicable Safe Harbor program;
 - ii. the Agent is governed by the 1995 EU Directive, EEA or Swiss data protection laws, or an equivalent law recognized by the European Commission as providing an adequate level of data protection; or
 - iii. the Agent has executed a written agreement with Brunswick requiring the same or higher level of privacy protection as set forth in this Policy.
- C. **Sensitive Personal Data.** Sensitive Personal Data shall not be collected, handled or processed without explicit prior consent from the Data Subject and advance approval from the Privacy Office, unless otherwise required by applicable law or except as described below.
- D. **Notification.** Employees should contact the Privacy Office with questions or complaints regarding data security, the handling of Personal Data or Sensitive Personal Data or Data Collection Points.
- E. **Compliance.** Adherence to the Safe Harbor Principles (see below) is mandatory. Violations of this Policy may result in disciplinary action, up to and including termination of employment for Employees, or the termination of business relationships with contractors and consultants.
- F. **Self-Assessment.** Brunswick will coordinate self-assessments for compliance with Safe Harbor principles on an annual basis. Employees, contractors and consultants must provide assistance to facilitate audits if requested.

The Safe Harbor Principles

Individuals who process Personal Data on behalf of Brunswick must comply with the following Safe Harbor Principles:

- A. **Notice.**
- i. **Requirements for Notice.** Other than for anonymous or aggregated data, that is, data which does not identify an individual, Brunswick will provide the following information in clear and conspicuous language to each Data Subject from whom Personal Data is collected:
 1. the purpose for the collection of the Personal Data (for example, see the "Purposes for Collecting Personal Data/Human Resources Data" below);
 2. how to contact the Privacy Office with inquiries or complaints;
 3. the types of Agents and Third Parties to which it discloses the Personal Data; and
 4. the choices and means that Brunswick offers Data Subjects for limiting its uses and disclosures of Personal Data.
 - ii. **When Notice will be provided.** Brunswick will provide notice when it first requests Personal Data or as soon thereafter as is practicable. Brunswick will also provide notice before using such data for any purpose other than the reason for which it was originally collected or processed. For Personal Data collected from Data Subjects before this Policy became effective, the following section describes the purposes for collection of this data:

Purpose(s) for Collecting Personal Data/Human Resources Data

Authorized personnel may use Personal Data for employment-related purposes including, but not limited to: (i) reporting and statistics; (ii) performance management and appraisal; (iii) recruiting; (iv) supporting mobility of personnel; (v) succession planning and talent development efforts; (vi) training; (vii) benefits processing; (viii) budgeting and forecasting; (ix) accounting and payroll processing; (x) financial disclosures; (xi) maintaining databases and providing IT support; (xii) ensuring compliance with Brunswick policies and Codes of Conduct, including, but not limited to, the Brunswick Ethics program and associated investigations; (xiii) hiring and termination; (xiv) human resources management; (xv) personnel management for Brunswick entities; and (xvi) complying with legal obligations.

- B. Choice. Brunswick provides clear and conspicuous notice and readily available and affordable mechanisms for Data Subjects to choose how their Personal Data is processed under certain circumstances. Data Subjects can opt out if their Personal Data is to be:

1. disclosed to a Third Party, except as explained in the Onward Transfer section below;
2. used for a purpose not compatible with the purpose(s) for which it was originally collected or for a purpose that was subsequently authorized by the individual.

If the Data Subject does not consent to the processing of his or her Personal Data under the circumstances discussed above (i.e., the individual opts out), the Personal Data cannot be processed for those purposes

- C. Sensitive Personal Data

- i. Sensitive Personal Data cannot be collected or disclosed unless the Data Subject affirmatively consents (“opts-in”) except as described below.
- ii. Data Subjects must also affirmatively consent if Sensitive Personal Data is to be used for a reason other than the purpose originally authorized.
- iii. Opt-in consent is not required if the disclosure is:
 1. required by law or legal process;
 2. necessary or appropriate to prevent physical harm, harm or loss to property or financial loss;
 3. in connection with an investigation of suspected or actual illegal activity or violation of Company policy.

- D. Onward Transfers

- i. Brunswick will comply with the Notice and Choice Principles (see above) before disclosing Personal Data to a Third Party.
- ii. Brunswick will only transfer Personal Data to an Agent if the Agent: i) has subscribed to the Safe Harbor program; ii) is subject to the EU Directive; iii) has Binding Corporate Rules; (iv) has signed a written agreement requiring the same or higher level of privacy protection set forth in the Safe Harbor Principles or is otherwise subject to the Swiss Federal Act on Data Protection or another finding of “adequacy” by the European

Commission.

E. Access

- i. Brunswick provides Data Subjects access to their Personal Data and will accommodate reasonable requests to correct, amend or delete Personal Data.
- ii. Brunswick may limit or deny access to Personal Data where providing such access is unreasonably burdensome or prohibitively expensive under the circumstances, or if otherwise permitted by the Safe Harbor Principles.
- iii. To obtain access to Personal Data, Data Subjects may contact Brunswick's Privacy Office.

F. Security

Brunswick maintains appropriate administrative, technical and physical safeguards to protect Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction pursuant to this Policy and the Brunswick data security procedures. Please contact the Privacy Office for more information.

G. Data Integrity:

All individuals and entities subject to this Policy must take reasonable steps to ensure that Personal Data they collect and/or process is relevant to its intended use, accurate, complete and current. Brunswick depends on Data Subjects to update or correct their Personal Data whenever necessary.

H. Enforcement:

- i. Brunswick has established policies and procedures for periodically verifying compliance with the Safe Harbor Principles.
- ii. Brunswick will conduct an annual self-assessment of its privacy practices before asking the U.S. Department of Commerce for Safe Harbor re-certification.
- iii. Data Subjects may file complaints with the Brunswick Privacy Office regarding the processing of their Personal Data. If a complaint regarding an alleged breach of the Safe Harbor Principles cannot be resolved through an internal process, Brunswick will participate with EU government/regulatory authorities to resolve it.
- iv. Brunswick will take steps to remedy any complaints or inquiries arising out of a failure to comply with the Safe Harbor Principles.

Limitation on Application of Principles

Adherence to these Safe Harbor Principles may be limited (a) to the extent required to respond to a legal or ethical obligation; (b) to the extent necessary to meet national security, public interest or law enforcement obligations; and (c) to the extent expressly permitted by an applicable law, rule or regulation.

Changes to this Policy

From time to time, this Policy may be revised and/or supplemented and appropriately posted and communicated. Employees should ensure they review the Policy with the most recent Revision Date.

Brunswick Privacy Office Contact Information

Email: privacy@brunswick.com

Telephone: 855-283-1103 (toll-free North America) or 847-735-4002

In writing: General Counsel
Privacy Office
1 N. Field Court
Lake Forest, Illinois 60045

If you would prefer to ask questions or contact the Privacy Office in your local language, please contact your local Human Resources representative or Finance representative, who will liaise with the Privacy Office.

Related Documents

1. Security Policy (I.01.01)
2. Classification of Controlled Data Policy (P.01.02)
3. Records Management Policy & Schedule (L.03.01)
4. Protection of Restricted Data Policy (I.01.10.00)
5. Brunswick's Safe Harbor certification(s) can be found at <https://safeharbor.export.gov/list.aspx>.

Policy Owner and Who to Contact

Policy Owner: Brunswick Privacy Office

Privacy Leader: General Counsel