

Policy No. 45

Global Privacy Policy

Purpose

Privacy laws regulate the way Jones Lang LaSalle Incorporated (including its majority-owned subsidiaries, collectively, the “Company” or “JLL”) collects, stores and uses personal information. JLL seeks to comply with all the relevant laws but also to adhere to the following principles:

- Collecting personal information properly;
- Using personal information responsibly;
- Keeping personal information safe;
- Maintaining accurate, current, and relevant information;
- Respecting people’s information rights; and
- Sharing, disclosing and transferring personal information securely.

JLL recognizes that personal information is a major corporate asset. However, collecting and using personal information can also be a liability, for example, where there is a data breach. Therefore, JLL expects all its employees to consider the responsible handling and use of personal information to be both a corporate and a personal objective.

Scope

This Policy applies to all officers, employees, and reporting entities of JLL. This Policy sets out the basic standards that are expected of anyone with access to the personal information that JLL is responsible for, regardless of who it is about or where it is located. This includes personal information about its employees.

This Policy is intended to be supplemented by the [Code of Business Ethics](#) and the related policies referenced in this Policy.

Statement of Policy

This Policy applies to all information that identifies, or can identify, a living individual. Some examples of personal information are set out below. The Company’s policy is to comply with all laws relating to the protection of personal information on a jurisdiction-by-jurisdiction basis. However, the Company will also implement good practice standards on a global basis. Personal information may be held electronically or in manual form, both of which are subject to this Policy.

The Company collects personal information for purposes including:

- ensuring that the Company complies with its statutory obligations;
- enabling the Company to communicate with, and to provide services to, its employees and clients;
- engaging with its contractors and third-party suppliers;
- enabling the Company to maintain accurate client, employee and other records;
- enabling the Company to administer Human Resources processes such as compensation, payroll, benefits, succession planning and recruitment of new employees;
- marketing to existing and prospective clients and maintaining client relationships; and
- facilitating the authentication and/or authorization of mechanisms required to grant access to, and permit the use of, the Company’s information technology systems.

Policy No. 45

Global Privacy Policy

Personal Information the Company holds may include:

- a name, identifying number, symbol, or other identifier assigned to an individual – e.g. a Social Security Number;
- any information that describes anything about an individual – e.g. an entry on a personnel record;
- any information that indicates actions done by or to an individual – e.g. a report of a misdemeanour;
- client business contact details;
- an online identifier such as an IP address if it is used to monitor an individual's behaviour – e.g. the IP address of a personal electronic device;
- any other information that indicates an individual's personal characteristics; and
- evaluations of an individual's performance.

Personal Information could be about:

- Employees - such as professional qualifications, remuneration and benefits; family and next of kin; health and disability information;
- Clients - such as contact details (business or personal), nationality and data collected as part of know-your-client due diligence; and
- Third Parties - such as tenants' contact details, sub-contractors' qualifications or contact details, credit agency information relating to tenants or information identifying visitors to the premises it manages for clients.

Sharing and Transferring Personal Information

The Company may transfer personal information to third party companies where this is necessary for business purposes, internal administration or personnel management purposes. The Company may also transfer personal information to third parties, including clients, where this is necessary for the provision of services to the Company. This may, for example, include information concerning an employee's proficiency in foreign languages or areas of work in which an employee has expertise. Such information might be on an employee's CV and some of this information could be used in a biography for a sales initiative. The Company will take reasonable measures to ensure, as a matter of legal requirement or good practice, that any third parties who receive personal information about our employees on our behalf (such as a pension scheme or benefits administrator) treat it in a confidential manner and only use it for the purposes authorized by JLL.

JLL's Handling of Employees' Personal Information

When a person joins the Company it will create a personnel record. This is in the Company's legitimate interests and is necessary in order to administer the individual's employment. The Company will only collect the information it needs and will give employees access to it in accordance with their legal rights.

From time to time information about employees may be transmitted to different legal jurisdictions. Some jurisdictions will have a higher level of regulatory protection for personal information than others, and personal information may be transferred to jurisdictions which have a lower level of regulatory protection than that present in the home country. However, JLL will put the necessary measures in place to ensure that any personal information that is transferred remains protected.

The Company will ensure, so far as reasonably practicable, that any person who has access to personal information will respect its confidentiality and will only process it for a legitimate business purpose and in compliance with instructions issued by the Company.

Policy No. 45

Global Privacy Policy

Each employee may at any time ask the Company (i) to correct inaccuracies in his or her personal information, to update it as individual circumstances change (such as marriage) or (ii) to have access to his or her personal information in accordance with their legal rights. Rights may vary according to jurisdiction.

The Company will only use personal information for legitimate business purposes.

The Company will only process information about an employee's physical or mental health (beyond recording sickness certificates submitted by the employee or on the employee's behalf) in accordance with the relevant law and individuals' rights.

Records Management

The Company will take reasonable measures to ensure that personal information is accurate, complete, and current. If an assessment, for example of an employee's suitability for continued employment, is based on information that proves to be incorrect – for example an inaccurate attendance record - then the assessment must be amended to reflect the facts.

Personal information should not be kept longer than is necessary for its intended purpose. This means that personal information should be securely destroyed, or erased, from the Company's systems when it is no longer required for business, statutory or regulatory purposes, or is out-of-date.

Website Privacy Statement

Where the Company markets or undertakes ecommerce activities via the internet on its websites, extranets or in other ways, it will place an appropriate privacy statement on the website or otherwise make such a statement available.

Security Measures

The Company will take appropriate security measures to safeguard personal information from the point of collection to the point of destruction and ensure that it is not deliberately or accidentally accessed or compromised in any way. The Company may conduct audits to ensure the appropriate security measures are in place to safeguard the personal information for which it is responsible.

Enforcement and Monitoring

Employees acknowledge that global corporate policies and the Code of Business Ethics allow for the limited personal use of the Company's communications systems. Breaches of such privileges, due to negligence, carelessness, or malicious intent may lead to disciplinary proceedings.

In order to ensure compliance with these requirements and subject to applicable law, the Company reserves the right to monitor communications. The Company will record and store communications where this is necessary to prevent and detect, or to investigate and detect, unauthorized use. Please refer to [Policy 14 \(Information Technology Use\)](#) for further information on enforcement and monitoring.

Administration of Policy

This Policy shall be administered by Global Legal Services. The Policy shall be subject to periodic review and revision as necessary or appropriate.

Legal Restrictions on the Application of this Policy in Particular Countries

We intend this Policy to apply to the Company on a global basis. However, if a provision of this Policy would violate an applicable law or regulation within a particular country, then we will consider that such provision is void and of no force or effect as to our employees or operations within that country.

Policy No. 45

Global Privacy Policy

EU General Data Protection Regulation (GDPR)

Our businesses in the European Economic Area (EEA) and those outside of the EEA which offer services to people within the EU, are required to comply with the GDPR. This introduces legal obligations for JLL and legal rights for individuals that may not be applicable outside the EEA. Further discussion on the GDPR is provided in Exhibit A.

Related Global Policies:

The Global Corporate Governance and Compliance Policies listed below form part of our wider Privacy and Data Protection Program and can be viewed on Connect.

- Policy No. 10 – Document and Records Retention Policy
- Policy No. 14 – Information Technology Use
- Policy No. 27 – Information Classification
- Policy No. 28 – Information Security Incident Response
- Policy No. 30 – Compliance with Laws Relating to the Company’s Public Web Site
- Policy No. 39 – Managing Confidential Information on Mobile Devices and Removable Media

Many of our regional and local operations may have country or region specific privacy and data protection policies or guidelines in accordance with local laws and business practices. These can be viewed on the relevant regional Connect site.

Restriction on Posting Company Policies

In order to ensure reliance on the official version of policies, this Policy shall not be copied, reproduced or posted on any Company website without the prior approval of Global Legal Services.

The official version of this Policy is located on the [Connect Global Policy Portal](#).

Revision History Date	Description
January 1, 2014	Policy issued
March 2016	Updated logo and changed references to <i>Connect</i> to intranet
May 12, 2017	Policy 42 (Privacy of Employee Information) consolidated into Policy 45.
May 18, 2018	Added information related to the EU General Data Protection Regulation.

Global Privacy Policy

EXHIBIT A

Additional information for JLL employees in the EEA

One of the most significant implications of the GDPR for JLL employees concern their rights, in particular that they are legally enforceable and that a complaint concerning those rights can be lodged with a national data protection Supervisory Authority or the Courts. This may not be the case in jurisdictions that do not have data protection laws equivalent to those in place within the EEA.

The most significant rights for individuals under the GDPR are:

- **Right to be informed:** this means high standards of transparency whenever personal information is collected; typically, this is achieved through a privacy notice.
- **Access to personal data:** JLL businesses in the EEA are required by law to give employees access to their personal information, subject to certain limitations that may vary on a national basis.
- **Rectification:** there is a right to have personal information corrected if it is inaccurate, and to make any third-party recipients of the information correct it too.
- **Erasure (right to be forgotten):** this is a right to have personal information erased if, for example, the retention of the information is no longer necessary. Note that this is a qualified right and does not apply if, for example, retention of the information is a legal requirement.
- **Restriction of processing:** this is a right to have personal information ‘put beyond use’, for example whilst a dispute over the content of the information is being resolved.
- **Data portability:** this is the right to have personal information (that an individual has provided to an organization in a common, machine-readable format) transferred easily to another organization.
- **To object:** the right to object to processing means that in some cases an organisation has to stop processing an individual’s personal data, for example for direct marketing purposes.
- **To not be subject to automated individual decisions (including profiling):** this right means that where a decision is made about an individual by, for example a computer algorithm, the individual has a right to human intervention and to contest the decision.

In addition, the GDPR’s principles place certain obligations on JLL businesses. These include the need to have a specific legal basis for processing personal information, only collecting personal information where this is necessary for a particular purpose, keeping it secure and ensuring it remains properly protected if it is transferred outside the EEA.