



JLT EB PRIVACY & SECURITY STATEMENT

February 2018
Version 1.1 (processor to processor)





JLT PRIVACY AND SECURITY STATEMENT

PRIVACY STATEMENT

At JLT Employee Benefits (JLT) we know how important privacy is to you, your clients and your staff. So we've created this privacy statement to explain our approach to handling, storing and transferring personal data you provide to us and which we collect and process on your behalf. With the introduction of the Europe-wide General Data Protection Regulation (GDPR) in May 2018, we've reviewed what we do and how we do it, so you can be confident that we're properly protecting this information.

This privacy statement is supported by a detailed **security statement**. The **security statement**, at the end of this privacy statement, explains exactly how we protect your data and the systems we have in place to keep it safe.

Context

You are a **Processor** under the GDPR, which means that you process Personal Data on behalf of another party. That other party, who may be a **Controller**, decides why and how you process that Personal Data.

Under the GDPR, we're a **Processor** in the context of our relationship with you, which means we process Personal Data for you (your Personal Data), in line with what you ask us to do. Sometimes we may also have a legal obligation to process it.

Our privacy principles

We stick to some simple, strict privacy principles when we process your Personal Data and everyone at JLT follows them. When it comes to your Personal Data, we:

- process it lawfully, fairly and transparently. We'll get your consent to process data whenever we need to;
- collect it for a legitimate reason, tell you why we're collecting it and what we're going to do with it. We don't do anything more with the data beyond this;
- make sure what we collect is adequate, relevant and is only what's necessary for the reasons we've explained. If we can do the same thing without collecting Personal Data, then we won't collect it at all;
- do what's reasonable to keep it up-to-date, or, if it's inaccurate, out-dated or wrong, we delete it;
- only store it for as long as we need to process it and when we store it, we'll follow our document management retention policy;
- process it in line with the Data Subject's rights;
- process it so it's kept confidential, secure and available. This includes protecting it against someone accessing it without permission. It also includes keeping it safe so it doesn't accidentally get lost, damaged or destroyed;
- will only transfer it to countries outside the European Economic Area (EEA) in line with data privacy laws.

Definitions

Data Subjects – People whose information you and we, on your behalf, process.

Personal Data - Any data that relates to an identified or identifiable living individual. This includes, for example, information such as name, address, telephone number, email addresses, date of birth, bank account details and National Insurance number.

Special Category Data - Categories of information that require enhanced protection measures. This includes, for example, health related data about an individual.

Your Personal Data - The personal data and the special categories of data that you've given to us or which we collect and process on your behalf.

Processing – Any set of actions which is performed on Personal Data such as collecting, recording, organising, structuring, storing, altering, retrieving, using, disclosing or destroying.

Controller – The person or body that determines the purposes and means of processing.

Processor – The person or body that processes Personal Data on behalf of the Controller.

How we deliver on our principles and obligations

A policy of privacy – by design and default

We work on the principle of ‘privacy by design and default’. We’ve reviewed and redesigned how we process your Personal Data – we only process what’s necessary for us to deliver services and only hold onto it for as long as we need to. By default, we only make your Personal Data accessible to those who need it. When we bring in new systems or processes, or change existing ones, these principles are central to how we work.

Keeping our staff up-to-date

Everyone at JLT has a responsibility to protect your Personal Data. At least once a year, we train our staff on how to meet their obligations. And our staff and third parties have to keep your Personal Data confidential, not only while they work for us, but also after they leave.

If someone contacts us asking for your Personal Data, we take reasonable steps to check their identity before we share it.

Our organisational and technical approach

We’ve put in place appropriate, risk-based, organisational and technical measures to keep your Personal Data safe. Our security statement explains in detail how we do this.

Data Privacy Impact Assessments (DPIAs)

We carry out DPIAs to make sure that our processing of your Personal Data doesn’t create a high risk to the rights and freedoms of Data Subjects.

Complying with an individual’s rights

As your Processor, when one of your Client’s Data Subjects exercises their rights, we have a contractual and legal obligation to help the Controller to meet those rights. If one of your Client’s Data Subjects contacts us directly, we’ll pass this request on to you or the Controller, as agreed with you in advance, so that the Controller is in control of the response. We will help the Controller to meet their Controller Data Subject Rights obligations. In particular, we’ll give you or the Controller any information we have that they may need to respond to a request. If we have outsourced any processing to a third party, we will work with them to provide the Controller with the assistance they need.

Data Subject Rights

- Right to access;
- Right to rectification;
- Right to erasure (also known as the “right to be forgotten”);
- Right to restriction of Processing;
- Right to notification regarding rectification or erasure of Personal Data or restriction of Processing;
- Right to receive a copy of Personal Data in order to transfer it to another provider;
- Right to object to Personal Data being processed in certain circumstances;
- Right not to be subject to automated decision-making and profiling using Personal Data; and
- Right to withdraw consent.

Being transparent and giving notice

We know the Controller is legally obliged to be transparent with their Data Subjects and accordingly they will need to tell them (amongst other things) what Personal Data about them they process, why they process it, who they share it with and if any of their Personal Data is processed outside the European Economic Area (EEA). Where we’re processing Personal Data for you as part of the service we provide, all of this information is included in our contract with you.

What happens if something goes wrong?

We've put in place measures to spot potential Personal Data breaches. At least once a year, we give our staff training on how to spot a breach and how to deal with incidents if they happen. Through our procedures, we give suspected and actual breaches our urgent attention. If someone identifies a Personal Data breach (including one that looks probable, but isn't confirmed) they must report the incident to our Data Protection Officer as soon as possible. And, in our contracts, we also require all third parties who process your Personal Data to report any breaches to our Data Protection Officer as soon as possible.

We will inform you without undue delay if we become aware of a Personal Data breach that involves your Personal Data that may result in a high risk to the rights and freedoms of Data Subjects.

Transferring your Personal Data

We only transfer your Personal Data outside of the EEA in compliance with applicable data protection laws.

When we have to disclose your Personal Data

Sometimes we have to disclose your Personal Data to other people, when it's not part of the service we normally provide for you. We only do this if we're required to:

- by statute, a regulator, or by order of a court; or
- so we can get legal advice; or
- for legal proceedings; or
- for safeguarding national security.

Finding out more

The Data Protection Officer for JLT Employee Benefits is Mark Wicks.

You can contact him at Mark_Wicks@JLTGroup.com or 01344 464 496.

Still have a question?

If you have any questions, please get in touch with your usual JLT contact, who will be happy to help.



JLT PRIVACY & SECURITY STATEMENT

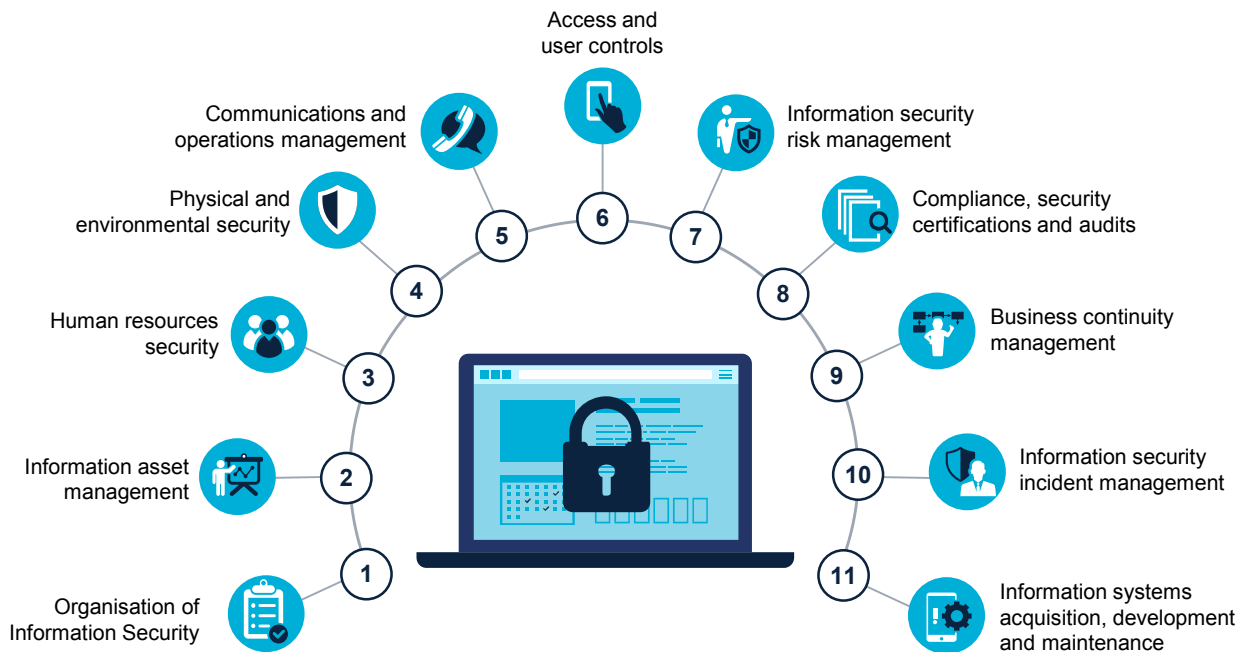
SECURITY STATEMENT

We take data security seriously. To reflect this, we've put in place a clear chain of responsibility when it comes to security. Our JLT Group Chief Information Security Officer (CISO) and CISO office is responsible for helping all JLT entities protect data and technology assets, and manage security risks. The CISO office does this by developing, monitoring and reviewing our information security framework policies and standards.

How we protect our data and technology assets

To check that the management of security is effective, all information security policies are produced and governed as part of the group-wide policy framework. We deploy these across the group through our Chief Operating Officer (COO) and Chief Information Officer (CIO) office structure.

We review our group information security policies regularly and publish them through the JLT group policy portal. These policies underpin a standard information security management system framework that we've designed across the following areas. You can read about each of these areas in detail below.



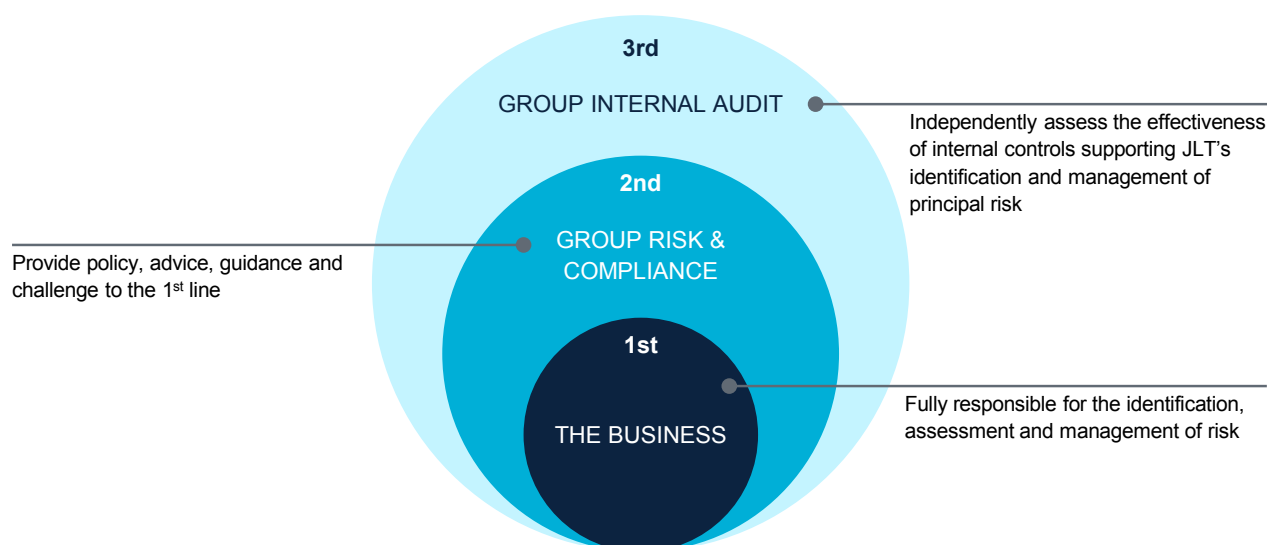
Our group information security policies are backed up by a formal set of standards. These standards set out the minimum requirements that our business units must meet when they implement controls to comply with this information security policy.

THE INFORMATION SECURITY FRAMEWORK AREAS



1 Organisation of Information Security

We have a JLT Group CISO who reports equally to the Group Chief Risk Officer (CRO) and the Group CIO. This is the second line of defence within our 'Three Lines of Defence' governance model.



Our Group CISO office oversees our business information security officers. These officers provide a more detailed level of support and are spread across all major geographic regions.

The Group CISO also works within the group governance model to make sure that the following teams understand our security risk position:

- The Group Executive;
- The Group and Business Board;
- The Group Operating Committee; and
- The Group Audit and Risk Committee.



2 Information Asset Management

As regulation has evolved, we've put a formal categorisation structure in place for our information assets across the group. We have four levels of classification and these apply at a user level and a company level. You can see this structure in the table, below. It supports the control design, security needs and handling of information assets throughout their lifecycle.

Classification	Public	Internal	Confidential	Highly Confidential
Examples	JLT Marketing Material	JLT Internal Policies and Procedures	All client data and all Personal Data that is not deemed highly confidential	Medical related information, trade union membership, mergers and acquisition information.



3 Human Resources Security

We know what an important part people play in terms of our cyber resilience and security capability. So we've broken our management of this issue into three areas:

Joiners and recruitment

We carry out standard checks and enhanced vetting, including CRB checks in the UK. We use financial sanction lists for anyone who might be a risk in relation to customer data or financial crime. We ask for educational certificates and verify any details of training from previous employers. And we'll ask people to fill in any details if there are gaps in their CV.

Training and information security awareness

During inductions, we tell our staff all about our information security policies and how important they are. And our employee handbook reinforces their roles and responsibilities. We run mandatory annual online refresher courses and use other tools, like phishing tests.

Role changes and leavers process

We have a formal joiners / movers / leavers policy and process in place and we use automation technologies where we can. This includes direct management oversight and accountability to ensure their employees only have access to data that they need for their role and that all security steps are followed when they leave.



4 Physical and Environmental Security

We've broken down our approach to physical and environmental security into three broad categories:

Data centre security

We follow the ANSI tier 3 industry standard, providing n+1 power, redundant cooling and 24/7 security with connectivity to a wealth of technology partners and providers. We use world class co-location facilities operated by well-known and respected global data centre providers. These facilities conform to all the normal industry standards and best practices for data centres. This includes full perimeter security, 24-hour security guards, electronic access controls, access logging and physical segregation between tenant areas within the machines rooms. Access to sensitive areas is logged electronically. If needed, our property services and security team can review these logs. And all server rooms and data centres have CCTV.

JLT office security

We secure entry and exit points at our locations. We give our employees access passes when they join, with their name and photo. Only authorised people can give others access to our offices. We keep a log of who accesses any sensitive areas. And our property services and security teams can review these logs if they need to.

Third party services security (including the cloud)

As part of our third party risk management framework we conduct information security due diligence on third parties. We look at the potential information security impacts associated with the service they're providing. In turn, this determines the level of detail and assurance we collect. We assign relationship managers to monitor our key suppliers and make sure we have on-going governance in place. And we set out all of our third party security requirements in our service delivery agreements.



5 Communications and Operations Management

We follow industry best practice design principles for our platforms and networks. And we use the Information Technology Infrastructure Library (ITIL) industry-standard framework for communications and operations management. This covers all phases of our service design, service transition and service operation. There's a comprehensive set of information security standards and procedures within that framework, including:

Protection of communications links

Private network access: We use Virtual Private Network (MPLS) technology with secure tunnels to provide office and data centre connectivity. We control LAN access at the port level and WIFI access by physical device ID.

Remote network access: We use 2-factor authentication to establish a secure connection to access services on the company LAN. Laptops can establish a secure link using the same system.

Protection of data in motion, at rest and data leakage controls

We look to encrypt data in motion and secure data at rest. We do this as a security design principle, assuming there are no technical limitations. We achieve this through a standard set of methods and technologies, which are dependent on the sending and receiving systems involved with transferring that data. All of the systems are based on industry standards and best practices. For data at rest (bearing in mind any technical limitations), we deploy encryption technologies at the hardware (including tapes and other removable media) and data storage layers.

We've put in place policies and standards to govern the transfer of data. This includes a broad data loss protection capability that uses both blocking and alerting methods. This capability is based on underlying technology capabilities, governed policies and rule sets.

We've made write access to removable media a controlled process.

General user controls

All of our employees, contractors and temporary staff are subject to a group-wide, all-employee, information security policy. This covers the acceptable use of technology resources, as well as rules for using approved technology solutions and services.

We've built our user devices to standard images, following good industry standards. And all of our laptops have full-disk encryption by default.

Hardening and patching controls

We manage all of our workstations and servers with a standard build. This includes installing software management agents which make sure any patches are deployed at the right time. The anti-virus (AV) patterns

are updated automatically and we use a central management console to track and report on compliance of devices.

All of our servers, including application servers, have AV installed and are appropriately configured. We update patches and we have an emergency out-of-bounds change and release process to deploy any critical or urgent security updates and patches.

Security logging and monitoring controls

As well as monitoring data traffic coming into our estate by way of checkpoint firewall, we use a security information and event management (SIEM) solution with agents on all critical servers that constantly monitor for suspicious activity.

We receive reports of any attempted attacks on the network with full details of threats attempted to be exploited, along with IP listings.

Anti-malware controls

We have an industry-standard anti-malware/anti-virus system in place. We update it at least daily, or more often, if necessary.

We monitor, filter and govern how our people use the internet, using industry-standard solutions. And we've put in place an acceptable use policy.

Vulnerability scanning and penetration testing controls

We run scans to test for internal vulnerabilities. And we carry out penetration testing on our internet-facing applications at least once a year.

We subscribe to a number of vulnerability notification services including membership of the CiSP portal provided by the UK NCSC, as well as the official hardware and software manufacturers' feeds. We routinely apply patches, in line with the hardware and software manufacturers' recommendations. All of these patches are subject to our change management process for approval and testing, and when we apply the patch depends on how severe the defect is. We assess and grade each patch in terms of severity and implementation timescales.



6 Access and User Controls

We know how important clear and robust identity and access management is. In particular, we recognise the part it plays in the confidentiality, integrity and availability of data. So, we've put in place policies for each of these areas:

Identity management

We manage our employees through our HR systems and processes to make sure we have unique identification in place. Because of this, we can interface with IT procedures, authentication processes and, where possible, identity and access management technology. This helps us to manage user accounts in a timely and appropriate way.

Authorised access and recertification

If someone wants access to our systems and applications, they need to make a request for a line manager to authorise. We give this access on a 'least privilege' and 'need-to-know' basis. And we recertify access to any systems that contain sensitive information. How often we review this access depends on how sensitive the information is.



7 Information Systems Acquisition, Development and Maintenance

We have put in place structured processes to look after the acquisition, development and maintenance of information systems.

For systems acquisition governance, our control and approval sits across the three primary layers of CIO, Chief Operating Officer and Chief Financial Officer. These people are also involved during the development and maintenance phases.

Where we develop the software ourselves, we follow a structured software development lifecycle (SDLC), which we've split into two broad sections. And we've included quality control checkpoints to govern the process.

Structured software development lifecycle Pipeline and demand management



SCOPING:

We follow a robust up-front scoping and planning phase with agile development techniques to create a delivery roadmap. We also make sure that our system analysts and architects work closely with the product owner.

Release planning and delivery



REFINEMENT:

Once we've understood the requirements and estimates in detail, we put together a release plan.



DEVELOPMENT:

We turn the release plan into a release candidate. We use detailed design and development to create the solution and then confirm that it's ready for testing.



TESTING AND VALIDATION:

We use independent regression, performance and functionality testing to make sure that the release is ready for the customer.



LAUNCH:

We offer support once we've released the solution.

We maintain separate environments for test data. This stops anyone getting unauthorised access to information assets, or making changes to those assets.

In terms of maintenance and decommissioning, we follow standard practices that embed and integrate with our ITIL-aligned service model. These connect with the communications and operations management area of the framework.

Specifically, for the decommissioning phase, we've put the following controls in place:

- We dispose of any equipment securely, basing our process on the Waste Electrical & Electronic Equipment Regulations 2013. In terms of equipment destruction, we wipe any tapes then overwrite them, using our tape backup software. When we destroy any media, including tape and drives, we use a rigorous destruction process. This process is based on (IL6) of the HMG Infosec 5 Standard Manual 'S'.
- We record any hard drives, then store them securely, following a data de-classification process. We process the procedure using UK Government-approved equipment and secure HDD & DLT granulation to 3mm. This process destroys the hard disk drive and makes it impossible to retrieve any data.



8 Information Security Incident Management

Information security incident management is an embedded part of our ITIL-aligned service model.

It makes use of the procedures, capacity and tools that we have to deliver that model. We have dedicated security operations resources and specific security incident and event management tools.

STEPS WE TAKE IN A SECURITY EVENT



In parallel to the main process, for major security incidents, we put in place connections with our wider data breach and business continuity policies. This includes communication, analysis and documentation of the incident.



9 Business Continuity Management

Our approach to business continuity management and disaster recovery is supported by a group-wide approach to risk management, including business impact analysis. When it comes to security, we focus on two primary controlling factors:

- We locate our disaster recovery systems and services in a geographically diverse, on-premises data centre with redundant power, cooling and security facilities. This gives us high availability and protection 24/7.
- Our technology major incident management process is part of the group's business continuity framework. We've embedded information security (including cyber security) into our crisis management, business continuity and disaster recovery planning.



10 Compliance, Security Certifications and Audits

As a company regulated by the Financial Conduct Authority (FCA) audit, compliance and governance are at the heart of our operations. We're subject to regular independent financial and IT system audits by both internal and independent third party auditors.

We are Cyber Essentials certified and we align our Information Security Framework (ISMS) with ISO 27001. We also carry focused ISO 27001 certification within targeted business areas.

We make sure that all key IT service providers are secure and compliant. As part of our vendor management and third party risk management framework, we assure security alignment through auditing, inspection and the review of certificates and reports (such as SSAE 16 SOC 1 or SOC 2 type ii).



11 Information Security Risk Management (including cyber threat management)

For us, cyber risk is a board level issue. We regularly focus on information security risk through our group governance committees.

We take a technology and behavioural approach to cyber security, because of the nature, scale and complexity of the threats it poses. Because of this, our approach includes adopting industry good practice for IT security controls, process and policy, supported by training and awareness. Our cyber framework is based on ISO 27001 and the NIST cyber security standards, which are endorsed by the UK and US governments.

We also recognise that insurance is an important part of managing cyber risk. We have specific cyber insurance cover and we also augment that with retained partner arrangements for cyber legal and cyber forensics expertise and support.

JLT Employee Benefits

The St Botolph Building
138 Houndsditch
London EC3A 7AW
Tel: +44 (0)207 895 7892

www.jltemployeebenefits.com

JLT Employee Benefits. A trading name of JLT Benefit Solutions Limited. Authorised and regulated by the Financial Conduct Authority. A member of the Jardine Lloyd Thompson Group.
Registered Office: The St Botolph Building, 138 Houndsditch, London EC3A 7AW. Registered in England No. 02240496. VAT No. 244 2321 96

© January 2018 276336