LHT GENERAL DATA PROCTECTION REGULATION POLICY

WHAT IS General Data Protection Regulation?

The EU General Data protection regulation (GDPR) is a European regulation EU 2016/679 which replaces the Data Protection Directive 95/46/EC and was designed to strengthen data protection of all individuals within the European Union. Individual rights are the same as under the Data Protection Act 1998 (DPA), however individual rights have been strengthened. The general data protection regulation will, considerably extends the current requirement of the DPA (1998) to reflect the advancement in technology.

When will the new G DPR come into effect?

General Data Protection Regulation comes into effect on 25th May 2018. A new data protection bill will be implemented GDPR standards across all data processing within the EU. All personal data has to be protected

This policy focuses is to assist the implementation of a new way of processing individual's data to ensure that LHT is compliant, this will include reviewing LHT current policies, procedures, employment contract and privacy notice. Under General Data Protection Regulation 2016 the lawful basis for processing individuals personal data are:

- Consent
- Legitimate Interest
- Contract
- Protection of Data
- Processing for employment purpose
- Processing of the provision of health and social care services.

Brexit and Data Protection Bill

The UK is due to leave the EU on UK's data protection regulation will remained interconnected with that of the UK. The UK is due to exit the EU on 29th March 2019, until the UK actually ceases to be a member state of the UK, GDPR will have a direct impact in the UK and will be legally enforceable against UK businesses.

Jurisdiction Impact- GDPR IS applicable to organsiation and employees outside the UK who offers goods or services to individuals. The trigger of GDPR is linked to whether the data being collected is about an EU individual, or has the potential to identify individuals who are in the EU, rather than the location of the business,

Government- The UK government acknowledges the need to continue free flow of data between the UK and the EU post Brexit.

The information commissioner's Office (ICO) has not yet published an update version of its guidance for employers to reflect the new requirements of the GDPR, and has not provided a date when they are likely to do so. The previous Employment Practices Code is still available on the ICO website, as well as the detailed supplementary guidance to accompany the Code, be aware that some parts may be out of date and can no longer be dependent on for examples employee consent to data processing.

Glossary of Key terms

Understanding key GDPR key terms

Data Controller

The Data controller/ employer determines the purpose and means of processing of personal data relating to employees.

Data processor

Individuals who process data on behalf of the controller, such as payroll provider, is constituted a data processor.

Data Subject

The individual whom the data relates to, or anyone who within the boundaries of the EU boarders of he EU at the time of processing their data.

Automated Decision-Making (ADM):

Data Protection Principles:

General Data Protection Regulation update the principles of the DPA (1998). The objective of the principles is to protect individual from infringement of their privacy that can cause detriment.

London Housing Trust will need to ensure that they receive consent from staff and clients and external agencies to process personal data, and that personal data is processed in accordance with the data protection principles. LHT will need to comply with the six principles below to ensure that the company are processing personal data lawfully. The principles are summarized below:

1	**Article (5) of the GDPR requires that data be processed Lawfulness,& transparency processing**	Ensure that LHT have a legal grounds for carrying out the activity and that personal data is processed lawfully, fairly and in a transparent manner. Tell the clients and employees what information you hold about them.

		not use personal data in a way that has an unjustified adverse impact on the employee (it can have an adverse impact, as long as it is justified)
	Obtain personal data for specific, and explicit and legitimate purpose	Personal data will only be collected for a specified, explicit and legitimate purpose. If the company wished to use information other than for the stated purpose , LHT will need to take into account the following facts to ascertain whether the new purpose is compatible with the stated initial purpose: • Is there a correlation between the new and old purpose? • The relationship between the parties • Type of data , does it fall under special category • What contingency is in place to prevent mis-use
2	Data minimisation	LHT will only process personal data where it is adequate, relevant, and limited to what is necessary for the purpose of processing. The company will not retain data longer than they need in order to meet the purpose for which the data is held
3	Data Storage	LHT will implement measures to ensure that personal data is secure and take steps to ensure that it is not lost, destroyed or damaged and is available on a need to know basis. The company will also ensure protection against unauthorised or unlawful processing.
4	Accuracy	LHT will ensure that the details recorded are accurate and take all steps to ensure that inaccurate personal data is amended or deleted without delay
5	Confidentiality	Personal data must be processed in a manner which ensures its appropriate security
6	Accountability	The Data Protection Officer is responsible for, and must be able to demonstrate compliance with the data protection principles.
7	Compliance with Principles	The GDPR introduces a new concept of 'demonstrable compliance' or the 'accountability principle' which means that it is not enough for you to comply with each of the principles set out above; you must also be able to demonstrate that you do.

What are the lawful basis for processing

LHT staff members who need to process individual data should ensure that prior to processing clients or staff data, the company consider the lawful basis before commencing to process personal data. It is crucial that consent is obtained from the individuals. (see consent on page7}

The lawful basis for processing employees and clients data will depend on the specific purpose and context of processing. In some case more than one lawful basis may apply. LHT must ensure that they have a valid basis in order to process clients and staff data, LHT should also ensure that all lawful basis are documented . To ensure compliance we will consider a variety of factors:

- LHT will consider the following , what is the purpose – why do the company need the data
- Whether LHT can achieve an outcome/ process application for housing without the data and what other means can LHT achieve the outcome.
- Can LHT have a choice , whether or not to process the data .

See checklist in appendix

Section 2

What is Personal Data?

Personal data is any information that relates to an individual who can be directly or indirectly identified from that information. Identifiers includes: persons name, identification number, location data, or online identifier, will impact on the manner in which organization collect data.

The General Data Protection Regulation applies to both automated personal data and to manual filling systems where personal data is accessible according to specific criteria, This could include chronologically ordered sets of manual records containing personal data.

What information does LHT have to provide

Where personal data is collected directly from the individual, LHT will provide the following information:

Contact details of the Data Protection Officer (DPO) where applicable

Inform the individual the purpose and legal basis for collection the personal data

The length of time LHT will retain/store your personal data

Sensitive data

Article (9) of GDPR refers to sensitive personal data as 'special categories of personal data Sensitive personal data includes: ethnic origin, political opinion, religious or philosophical belief, health, sexual orientation, data relating to criminal record conviction and offences, and information relating to criminal

allegation proceedings and biometric data, is afforded special protection. Financial data however, is not considered sensitive data. LHT decisions as well as the lawful basis the company referred to in relation to compliance of GDPR/

Examples of sensitive data;

- Racial or ethnic origin
- Bio data details
- Trade Union membership
- Sexual orientation
- Physical and mental conditions

Types of Sensitive Data LHT may hold:

- Sickness records, per-employment medical questionnaires, drug and alcohols test
- Equalities opportunities monitoring form
- Payroll information,
- Private health insurance records. Which may contain information relating to an individual sexual life, etc.

Criminal record data (see article 10)

Criminal data is defined as information held about an individual criminal convictions ad offences, and information relating to criminal allegations and proceedings. When processing criminal conviction data or data relating to criminal offences LHT will ensure that the company identifies both a lawful basis for general processing and additional condition for processing this type of data in accordance with Article 10. To comply with the above Article LHT will instruct staff and monitor processes to ensure that the lawful basis for processing criminal offence data is documented to ensure accountability.

Anonymisation and pseudonymisation

Data will only be considered anonymised under the GDPR if the anonymisation is done in such a way that the data subject is not or is no longer identifiable. This means that the data must be stripped of any identifiable details, making it impossible for anyone to derive any information about a particular individual, even if combined with additional information that the data controller or a third party possess.

Properly anonymised data falls outside the scope of the GDPR and you can therefore process it however you wish. However, true anonymisation is very difficult to achieve.

Employers who remove names and other individual identifiers from information about employees – for example, to prepare and analyse absence statistics across the organisation, or to provide information to

a potential purchaser in a business acquisition – are more likely to be pseudonymising that data (i.e. altering it so that a particular individual can no longer be identified without the use of additional information). Personal data that can be pseudonymised – eg key codes can fall within the scope of the GDPR depending on how difficult it is to link the pseudonym to a particular individual.

It is important to note the distinction between anonymised and pseudonymised data because pseudonymised data is still personal data, and therefore subject to the requirements of the GDPR.

However, the pseudonymisation of personal data is viewed positively under the GDPR, both as a means of protecting individuals' rights and as an appropriate measure for ensuring the security of personal data.

Activities covered by GDPR/

The primary activity covered by the general data protection regulation is processing of personal data manually or automatically which forms part of a filing system or is intended to form part of a filing system.

LHT will need to disclose the following to staff and clients:

- Why LHT is collecting staff and client data
- How the individual data will be processed and their legal basis to process the data.
- How the individual data will be stored
- LHT will also carry assessment to ensure equilibrium between the organization needs and the rights and freedom of the individual.

Consent

In compliance with GDPR, LHT has processes in place to ensure that consent sought is freely given by applicants to process their data, the consent received should be specifically for the purpose for which LHT wishes to process the personal data. Pre ticked boxes often used no longer be sufficient.

Consent means offering individual an informed choice and control. If consent is genuine consent will be evident whereby individuals decides whether they wish to participate in the process, it will build trust and engagement, and enhance the organization reputation. Consent mu

- Consent requires positive opt-in. Don't use pre –ticked boxes or default consent.
- Explicit consent required a very specific statement of consent/or expressed in words
- Consent should include the controller's name, the purpose of the processing and the type of processing activity.
- When requesting consent be clear and concise.

- Inform individuals that they have the right to withdraw their consent at anytime.
- Do not make consent a pre-condition of service.
- Evidence of consent must be kept including, who, when, how, and what you communicated to people.

Consent request should be separate from the terms and conditions of the LHT, and should include the following:

- The company name
- The third party who will rely on the consent
- Why you need the data
- What you will do with the data
- That the individual can withdraw consent at any time

Consent check list

for further information refer to ICO web page using the link aside consent.

To Protect the Well-being/Health of an Individual

GDPR consent may not be necessary in cases whereby a member of staff or client may be at risk, for example in cases of life and death for example the provision of emergency medial care. If the individual is capable of giving consent the processing will not apply.

Special Categories (Art)

In many cases explicit consent will be required, there are however a number of situations such as in the case of health and social care sector consent may not be required. Examples where explicit consent may not be required,

- processing in the field of employment
- Processing is required for HR purposes

What is Processing

Processing entails any operations that LHT carry out on personal data which includes:

- Collection
- Recording
- Storage

- Alternation
- Retrieval
- Consultation
- Use
- Disclosure
- Dissemination

Processing

Legal obligation

Legal obligation provision for specific processing, for example processing personal data to comply with the legal obligation to HRMC in terms of disclosure of employees pay. In the event that this is challenged please refer the individual to the relevant government website.

Court order may require LHT to process personal data this also qualifies as legal obligation

A retail energy supplier passes customer data to the Gas and Electricity Markets Authority to comply with the CMA's Energy Market Investigation (Database) Order 2016. The supplier may rely on legal obligation as the lawful basis for this processing.

If you are processing on the basis of legal obligation, the individual has no right to erasure, right to data portability, or right to object. Read our guidance on individual rights for more information.

There is a specific condition at Article 9(2)(c) for processing special category data where necessary to protect someone's vital interests. However, this only applies if the data subject is physically or legally incapable of giving consent. This means explicit consent is more appropriate in many cases, and you cannot in practice rely on vital interests for special category data (including health data) if the data subject refuses consent, unless they are not competent to do so.

Processing lawfully – controller obligations

In addition to requiring you to comply with the data protection principles outlined above, the GDPR imposes further specific obligations on you as a data controller/employer. These are described briefly below.

Obligation	**What it means**

Provide fair processing information	Linked with the principles of 'fair, lawful and transparent processing' and 'obtaining personal data for specified, explicit and legitimate purposes', the GDPR requires you to provide individuals with detailed information about what data you collect, the purposes for which you collect it, and how long you hold it for. We refer to the document in which such 'fair processing information' is provided as a 'privacy notice'
Respect and facilitate the exercise of individual rights	LHT will comply with by ensuring that their policies enable individuals to exercise their rights under the GDPR. Clear guidelines will be given how to request and their rights to make a Subject Access Request. All staff members will ensure that clients and the public are aware that they have a right to object to their data being processed.
Implement appropriate technical and organisational measures	LHT has appointed a Data Protection Officer, and listed the DPO details on on the privacy policy and consent letter. LHT has also You must put in place appropriate measures to: ensure your compliance with the GDPR; be able to demonstrate that compliance; and ensure an appropriate level of security for the data that you process.
Data protection by design and by default	LHT has implemented secure emails as a extra safegurard to ensure that the processing of clients personal data, is s integrating data protection into activities that involve processing personal data, from the design stage of a new process, and during processing itself.
Only use processors that provide guarantees of compliance	LHT has provided all staff with a employee privacy policy which they signed and returned. This will be attached to their personal file to ensure compliance with GDPR.
Maintain a record of processing activities	LHT have ensured that their policies include guidelines for retaining records of processing activities for staff and clients. LHT understand that we will process clients and employee health data, and other types of special category data. The time frame that various types of document will be kept is listed below. The record must include certain specified details of how data is processed and must be produced to the ICO on request.

Notify data breaches to the ICO and affected individuals in certain circumstances	In the event of any breaches LHT policy sets out clear guidelines and contact details what needs to be done and who will need to be contacted. Staff are aware that they need to contact the ICO of any data breach without undue delay (and, where feasible, within 72 hours of becoming aware of it), unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. Where the breach is likely to result in a *high* risk to the rights and freedoms of individuals, you must inform the affected individuals as well.
Conduct Privacy Impact Assessments (PIA) for certain types of processing	A privacy impact assessment was conducted to assess risk the "likely risk to the rights and freedoms of natural persons" (see appendix) The PIA highlighted risk minor risk. To comply with the GDPR requirement the company has taken measures to mitigate the risk to the processing and personal data. All records are now stored electronically.
Do not transfer data outside the EEA without ensuring an adequate level of protection	The organisation will not need to transfer information outside the UK in the event that a request is made to transfer data outside the EEA, the organisation will ensure that special safeguards in place. *You can find more guidance in Disclosing personal data to third parties.*
Appoint a Data Protection Officer (DPO) if required	A DPO has been appointed, who will be responsible for the interpretation and compliance of GDPR, as well as assist the organisation /(data controller). The DPO will report to the Board of Directors. The appointment of a DPO is obligatory under the GDPR for certain organisations: • LHT is a Non- Profit private organisation, our core activities consist of processing operations that require regular and systematic monitoring of the data subjects of special categories of personal data and data relating to criminal convictions and offences.

HR and data protection principles

London Housing Trust will update HR-related personal data expeditiously if an individual advises that his or her information has changed or is recorded inaccurately.

Personal data gathered during recruitment of staff, volunteers, apprenticeship will be held in individual personal file, hard copy will be stored electronically, on HRIS. LHT will hold HR related personal data for a period specified in the privacy notice to individual.

London Housing Trust will keep records of how it processes activities in respect to HR related personal data in accordance with the requirement of the General Data Protection Regulation.

HR are legally required to retain records for a minimum length of time,

Decision to retain information will rely on our retention policy

Contracts

Article 6 (1) (b) gives LHT a lawful basis for processing where: the processing is necessary for the performance of a contract to which the data subject is party or in order to process information for the data subject to enter into a contract.

LHT will have lawful basis for processing if:

- To process data for individual with whom the organization has a contract
- If LHT request a quote from a contractor for a prospective job and the organization need their personal data to process the action.

Retention Policy

retention periods for other HR data

The table below sets out examples of possible retention periods for employment-related records/personal data that an organisation might choose to apply having gone through the decision-making process summarised above.

Employment record	**Retention period**	**Reason for retention period of records**
Recruitment		
CVs/application forms, interview notes, written references from previous	6 months from date of appointment or confirmation that	The length of time is to provide LHT with sufficient time for purposes of verification re appointment of successful candidates and takes

employers and copies of qualification certificates for successful candidates	application unsuccessful	account of limitation period for potential discrimination claims from unsuccessful candidates - three months (plus margin for Early Conciliation or possible extension of time limit) *LHT will ensure that all candidates are made aware that the time frame that their application will be retained by LHT.*
CVs/application forms of unsuccessful candidates, kept to inform candidates of future vacancies	12 months from date CV/application submitted	Consent letter will be sent to each applicant, informing them that LHT wishes to retain their data, as well as giving them an opportunity to opt out. The consent letter will also inform the applicants that their CV/application will be shredded after 12 months, if they wish to remain on LHT register they should submit an updated CV before the end of the period. Candidates who do not consent to
Copies of qualification	LHT will retain all qualification submitted including those required for employment	Copies of certificates which expires, will not be kept by LHT, only valid qualification will be kept aside file as well as electronically.
Contract of Employment, Job description and statement of terms and conditions	Contract will be retained for the period of employment with LHT and six months following termination of employment. Where LHT notices the possibility of ER dispute relating to constructive dismissal or unfair dismissal the contract will be retained for at least six	The period of retention is linked to the time frame in which an employee can make a claim to the tribunal including 3 months to allow for early conciliation. Limitation period for breach of contract claims and equal pay claims is 6 years from date of purported breach

	months	
Absence Management		
Holiday records	A minimum of 2 years from end of holiday year in which the last holiday taken	The importance of keeping holiday records. Employees with variable pay elements may currently have claims in relation to holiday pay. Employers will need details of holiday taken to defend holiday pay claims. Retention period allows for scope for possible employment tribunal claim. LHT may decide to keep some employees holiday pay records for a longer period, if they believe they are at risk of lengthy back pay claims should the current legal challenge be successful. (For example, if variable pay has not historically been included in holiday pay).

Records relating to sickness absences (not pay), including • self- certification form • return to work interview/forms • GP Fit Notes • sickness absence management records	If no action taken by us further to your attendance management policy. LHT will retain the policy from the date of receipt to end of applicable rolling reference period to which your attendance management policy triggers apply (*e.g. 12 months)* Disability sickness absence in relation to the equality Act 2010 is not recorded under the normal sickness policy procedures and therefore does not invoke triggers. This relates to illness such as (cancer, ME, HIV/AIDs). Sickness that does not fall under the above will invokes trigger(s) in accordance to our attendance management policy and warning(s) given, this is done on a rolling 12 months from the expiration date of the 12 months period, including the most recent warning (which could be cumulative if attendance does not improve).	LHT will keep sickness absence record for operation of attendance management policy and to defend against claims arising from operation of attendance management processes – including unfair dismissal and disability discrimination. There is normally 3 months limitation period for employment tribunal claims, plus margin for early conciliation/claims out of time).

SSP records	3 years after end of tax year in which sickness occurred and SSP payments made	Notwithstanding that there is no longer a need to keep records of SSP– this was removed by the Statutory Sick Pay Regulations 2014. LHT will retain records in the event that HMRC decides to carry out an audit to check whether LHT is paying SSP correctly, and impose fines for SSP failings
Staff Performance Management		
Appraisals documentation	3 years from date of completed appraisal	Required for performance comparison purposes (including, if applicable, decisions that are linked to appraisals, such as redundancy selection and internal promotions - 3 years is likely to be the maximum period on which it would be fair to base such assessments)
Performance improvement documentation (further to the company's formal performance improvement procedures)	For the period during which performance is being assessed, plus 12 months thereafter	Employment tribunal claim limitation period (plus 3 month scope to allow for early conciliation/extension of limitation period, or in the event that the employee performance recurrence in performance.
Work-related training records	Dependent on nature/reason for training Training is essential and is required to demonstrate wider statutory/legal compliance (such as H&S . QAF, CQC and obligation or proper financial regulation) keep record of employee training for as long as necessary to demonstrate legal compliance.	Training is a crucial element to ensure that LHT staff are complaint and work within regulatory standards. LHT will therefore retain training records to demonstrate compliance with wider legal obligation and LHT policies as well as our commitment to equality and diversity.

Records of disciplinary investigations and procedures where no further action taken	Where no further action is taken following a disciplinary investigation LHT will retain records and will delete three months following the investigation. The employee will be notified of the deletion	There is no basis to retain documents for more than three months
Records of disciplinary investigations and procedures where further action taken/sanction imposed	If disciplinary lead to sanction the records will be kept for 12 months from date sanction during the employee tenure and six months following employee termination/resignation	12 month period based on 3 month limitation period for discrimination or unfair dismissal claim plus allowing period for early conciliation or any extension exceeding the statutory period.
Grievances – letters/investigations/ process and outcomes	12 months from date of completion of grievance procedure in the event the grievance relates to contract disputes or pay the records will be held for a minimum of 6 years	6 month period based on 3 month limitation period for discrimination or constructive unfair dismissal claim (plus allowing period for EC and possible extension of statutory period). Dispute re pay/contract terms – limitation period for Equal Pay claims Note: Some employers may decide to retain a brief record/note of the fact that a grievance was made and the final outcome for longer than their retention period for the full documentation relating to a grievance – to guard against 'serial' grievance raisers)
Subject Access Requests/exercise of other	12 months from date of request/exercise of right	Data controllers can refuse to comply with data subjects' rights if the nature of the request is

individual GDPR rights		'manifestly unfounded' or 'excessive' – which may be the case if the nature of the requests is repetitive
Redundancy - details of selection scores re employees not selected for redundancy	6 months from date of termination of those selected for redundancy	6 month period based on 3 month limitation period for discrimination or unfair dismissal claims by selected employees in relation to their selection (plus allowing period for EC and possible extension of statutory period).
Family leave		
Flexible working requests	Records will be retained up to 12 months from date of request in line with LHT policy.	LHT is policy clearly indicates that the organisation will only consider one application for flexible working per year (12 months period).
Record of family leave taken – maternity, paternity, adoption, shared parental (other than those re pay/as required by statute – see above)	12 months following return to work from applicable leave	To ensure employer complies with obligation not to treat employees less favorably/subject them to a detriment by virtue of their having exercised their right to take statutory leave
Employee Termination/Resignation		
• Letters of resignation/ dismissal • Notes of exit interviews • Record/audits of return of company property	Records will be held 6months following resignation or dismissal.	Employment tribunal limitation period is typically 3 months (plus leeway for early conciliation or extension of limitation period)

• Employee personnel file will be retained in accordance with a statutory obligation		
Information to enable you to answer reference requests about ex-employees, e.g. name/date of employment/position etc.	References will be provided for employees for a maximum of 2 years from date of termination.	In some circumstance LHT may agree to keep some minimal record of employment post-termination, such as name, date of employment and position in order that they can respond to future reference requests. The retention of such data will be agreed with the employee to ensure compliance with GDPR.

Client Records

London Housing Trust will update the dashboard where client information is kept promptly if a client or an external agency notifies a member of staff of changes to their circumstances.

Individual Rights

The new General Data Protection Rights has extended the rights of individual, they have a number of right relating to their personal data. LHT will need consent to process request, process and store personal data of their staff and clients.

- The right to be informed how their data is being processed and stored
- The right to access personal data held by LHT
- The right to have in accurate information rectified or if there is a dispute relating to legitimacy grounds.
- The right to request the erasure of personal data held by LHT if it being processed unlawfully
- The right to restrict/stop the processing of their personal data if the individual rights override LHT legitimate grounds for the processing of data wherein LHT relies on legitimate grounds for processing the data.
- The right to data portability, this is where data has been processed by automated means. This

includes automated recruitment process, on boarding or attendance management.

- The right not be subject to automated decision making.

Where an individual imposes a restriction in relation to the processing of their personal data, whilst LHT may continue to store the data, it is crucial that LHT only process the data under the following circumstances:

- With the individual consent
- To establish or defend legal proceedings
- For the protection of a right of another person
- For reason of important public interest

Subject Access Requests

Individual have a right to make a subject request. When an individual make a subject request LHT has to take into account the new GDPR rules. LHT will advise the individual of the following:

- Whether or not his/her data is processed and is so why, what type of personal data and the source from which to obtain the individual personal data if they have not collected the data from the individual.
- Be told who will have access to their personal data, and to whom their data will be disclosed
- How long LHT will store their personal data (as well as how they the period of storage will be decided for different category of personal data.
- LHT will provide a copy of the personal data undergoing processing. This will normally be in electronic form unless the individual agrees otherwise.
- Additional copies can be provided, however LHT will charge administrative cost to provide additional copies.
- When refusing and individual request for data access, LHT will advise the individual of their right to appeal

To make a subject access request the individual should send an email gdpr@londonhousingtrust or use the company data access request form. The person making the request, needs to provide a description of the data, the purpose of which it is processed,

LHT will ask for proof of identification before the request can be processed. LHT will inform the individual if they need to verify their identity and what documents they require.

LHT will normally respond to request within one month of receipt of the subject access. If LHT is unable to respond to your request within the specified time frame in accordance with the GDPR, they

will write to you to explain the reason for delay.

LHT reserves the right to refuse or charge for data which is defined as manifestly unfounded, or where the request is excessive. In exceptional cases where LHT decides to respond, LHT will charge a fee an administration fee which is based on responding to the request.

Data security

LHT is committed to ensuring high security of HR -related personal data. LHT has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure. LHT restricts the access to employee personnel files and access is only granted to the following staff members within LHT:

- LHT Board of Directors
- Data Protection Officer
- HR Advisor

All other access to employee personal files by the Senior Operational Manager are carried out under supervision to mitigate misuse or disclosure.

Data Protection Officer

LHT Data Protection Officer will be responsible for ensuring LHT complies with GDPR principles, LHT will need to :

- Implement procedure and processes to ensure compliance with GDPR
- Maintain the processing, recording and documenting
- Appoint a DPO

LHT does not have 250 staff and therefore do not need to maintain additional internal records of their processing activities.

Data breaches

Data breach is defined by ICO as a security incident that impacts on the confidentiality integrity or availability of personal data.

Article 87 of the GDPR requires all organisations to report certain types of personal data breach to the Information Commission Officer (ICO) within 72hrs of the breach to the Information Commission Officer. If the breach is likely to have detrimental impact on an individual rights and freedom, informing the individual of the breach is essential. Breaches includes:

- Access by an unauthorised third party

- Deliberate or accidental action by a controller or processor/ equipment failure.
- Sending personal data to a an incorrect recipient
- Computing device containing personal data being lost or stolen
- Alteration to personal data without permission
- Loss or available personal data

All staff members at LHT are responsible for staff should ensure that they are aware of data breach, how to report breaches.

Ensure robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant authorities.

Reporting Breaches

Personal data breaches includes, the loss of USB stick, data being destroyed, or sent to the wrong address, theft of laptop or hacking. Report breaches on (0303 123 1113).

Privacy and Electronic Communication Regulation (PECR), LHT uses electronic messages (internet) to send messages, LHT therefore must notify (PECR) of any breaches.

Unlawful use of personal data breach (Section 55)

LHT will need to report the breach using S55 of the Data Protection Act) to the ICF

Fines and Penalties for non-compliance of GDPR

There is a maximum fine of 2 percent of LHT turnover which can be applied where the following occurs:

- Failure to maintain records of processing activities
- Failure to appoint a Data Protection Officer.
- Processing data without consent of the data subject.

A maximum fine of up to 4 percent of LHT turnover can be applied if LHT fails to meet the following criteria:

- Failure of LHT to show that the data subject has consented to the processing of his or her data.
- Refusal to comply with Data Access, rectification, and erasure.
- Failure to provide subject with transparent information in concise manner.

LHT will provide training to all workers and volunteers about their data protection responsibilities as part of the induction process with on-line training Peninsula.

Individuals whose role require regular access to personal data, or who is responsible for implementing the policy, will receive additional training to assist them with their duties and compliance with the GDPR.

Appendix

Lawful processing Check list :

We have reviewed the purposes of our processing activities, and selected the most appropriate lawful basis (or bases) for each activity.

We have checked that the processing is necessary for the relevant purpose, and are satisfied that there is no other reasonable way to achieve that purpose.

We have documented our decision on which lawful basis applies to help us demonstrate compliance.

We have included information about both the purposes of the processing and the lawful basis for the processing in our privacy notice.

Where we process special category data, we have also identified a condition for processing special category data, and have documented this.

Where we process criminal offence data, we have also identified a condition for processing this data, and have documented this.

How to document LHT lawful basis?

The principle of accountability requires you to be able to demonstrate that you are complying with the GDPR, and have appropriate policies and processes. This means that you need to be able to show that you have properly considered which lawful basis applies to each processing purpose and can justify your decision.

You need therefore to keep a record of which basis you are relying on for each processing purpose, and a justification for why you believe it applies. There is no standard form for this, as long as you ensure that what you record is sufficient to demonstrate that a lawful basis applies. This will help you comply with accountability obligations, and will also help you when writing your privacy notices.

It is your responsibility to ensure that you can demonstrate which lawful basis applies to the particular processing purpose.

Read the accountability section of this guide for more on this topic. There is also further guidance on

documenting consent or legitimate interests assessments in the relevant pages of the guide.

ASKING FOR CONSENT CHECK LIST

- We have checked that consent is the most appropriate lawful basis for processing.
- We have made the request for consent prominent and separate from our terms and conditions.
- We ask people to positively opt in.
- We don't use pre-ticked boxes or any other type of default consent.
- We use clear, plain language that is easy to understand.
- We specify why we want the data and what we're going to do with it.
- We give separate distinct ('granular') options to consent separately to different purposes and types of processing.
- We name our organisation and any third party controllers who will be relying on the consent.

RECORDING CONSENT

- LHT will keep a record of when and how consent from individual was obtained
- Keep a record of exactly what the individuals were told at the time to obtain consent

MANAGING CONSENT

LHT will regularly review consent to check that the relationship, the processing and the purpose have not changed.

LHT has processes in place to refresh consent at appropriate intervals

Make it easy for individual to withdraw consent at anytime

Ensure that withdrawals of consent is done expeditiously

LHT will ensure through its policy and procedure that individual who withdraw their consent will not suffer and detriment.