LAPD ARCHITECTS PRIVACY POLICY

Introduction and Overview

lapd Architects are comitted to your privacy alongside the privacy of all our clients and persons we do business with. lapd will update this page as and when approportiate. This page was last updated on 30th May 2019.

This website is not designed for children and we do not knowingly hold or collect any data of anybody under the age of 18. When we collect your data we gather it specifically for the purpose of providing you with updates about the business of lapd Architects and correspondance related to your project enquiry. We use cookies in order to enrich your user experience online, and will use thrid party analytics and customization cookies , such as Google Analytics, in aggregate form to understand how the website is being used and to enhance user experience.

The following document is derived from our comprehensive in house GDPR compliance policy. This can be provided upon request.

What is personal data?

"Personal data" is any information relating to a data subject who can be identified (directly or indirectly) either from those data alone or by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that data subject. It excludes anonymised data, i.e. where all identifying particulars have been removed.

The data protection principles

Under the data protection legislation, there are six data protection principles that the Company and all members of staff must comply with at all times in their personal data processing activities. In brief, the principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency).
- Collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation).

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).
- Accurate and, where necessary, kept up to date; every reasonable step must also be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy).
- Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed (storage limitation).
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).

The Company is responsible for, and must be able to demonstrate compliance with, these data protection principles. This is called the principle of accountability.

Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

This principle means that both the Company and members of staff may only collect, process and share personal data lawfully and fairly and for specific purposes.

The data protection legislation provides that processing is only lawful in certain circumstances. These include where:

the data subject has given consent to the processing of their personal data for one or more specific purposes

the processing is necessary for the performance of a contract with the data subject, e.g. an employment contract, or in order to take steps at the request of the data subject prior to entering into a contract

the processing is necessary for compliance with our legal obligations

the processing is necessary to protect the data subject's vital interests (or someone else's vital interests)

the processing is necessary to pursue our legitimate interests (or those of a third party), where the data subject's interests or fundamental rights and freedoms do not override our interests; the purposes for which we process personal data for legitimate interests must also be set out in an appropriate privacy notice

The Company and members of staff must only process personal data on the basis of one or more of these lawful bases for processing. Before a processing activity starts for the first time, and then regularly while it continues, we will

review the purpose of the processing activity, select the most appropriate lawful basis (or bases) for that processing and satisfy ourselves that the processing is necessary for the purpose of that lawful basis (or bases). When determining whether the Company's legitimate interests are the most appropriate basis for lawful processing, we will conduct a legitimate interests assessment, keep a record of it and keep it under review.

Where the Company relies on consent as the lawful basis for processing, this requires the data subject to have given a positive statement, active opt-in or clear affirmative action; pre-ticked boxes, inactivity or silence do not constitute consent. If consent is given in a document that also deals with other matters, the request for consent must be clearly distinguishable and kept separate from those other matters. In addition, consent must specifically cover the purposes of the processing and the types of processing activity, so you must ensure that you obtain separate consents for different types of processing, where appropriate. Data subjects also have the right to withdraw their consent to processing at any time, they must be advised of this right and it must be as easy for them to withdraw their consent as it was to give it.

The data protection legislation also provides that the processing of special categories of personal data and criminal records personal data is only lawful in more limited circumstances where a special condition for processing also applies (this is an additional requirement; the processing must still meet one or more of the conditions for processing set out above). These include where:

the data subject has given their explicit consent to the processing of their personal data for one or more specified purposes; explicit consent requires a very clear and positive statement and it cannot be implied from the data subject's actions

the processing is necessary for the purposes of carrying out obligations or exercising specific rights of either the Company or the data subject under employment law or social security law

in the case of special categories of personal data, the processing relates to personal data which are manifestly made public by the data subject

the processing is necessary for the establishment, exercise or defence of legal claims

How is data stored and for how long?

Personal data must be collected only for specified, explicit and legitimate purposes and they must not be further processed in any manner that is incompatible with those purposes.

Personal data cannot be used for new, different or incompatible purposes from those disclosed to the data subject when they were first obtained, for example in an appropriate privacy notice, unless the data subject has been informed of the new purposes and the terms of this policy are otherwise complied with, e.g. there is a lawful basis for processing. This also includes

special categories of personal data and criminal records personal data.

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

We will only collect personal data to the extent that they are required for the specific purposes notified to the data subject. You must only process personal data where your job duties and responsibilities require it and you must not process personal data for any reason which is unrelated to your job duties and responsibilities. In addition, you must ensure that any personal data you collect are adequate and relevant for the intended purposes and are not excessive. This includes special categories of personal data and criminal records personal data.

When personal data are no longer needed for specified purposes, you must ensure that they are destroyed, erased or anonymised in accordance with the Company's rules on data retention and destruction set out below.

Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed.

The Company will only retain personal data for as long as is necessary to fulfil the legitimate business purposes for which they were originally collected and processed, including for the purposes of satisfying any legal, tax, health and safety, reporting or accounting requirements. This includes special categories of personal data and criminal records personal data. You must comply with the Company's rules on data retention and destruction set out below.

The Company will generally hold personal data, including special categories of personal data and criminal records personal data, belonging to clients, customers and suppliers for the duration of our business relationship with them.

Once our business relationship with a client, customer or supplier has been terminated, we will generally hold their personal data, including special categories of personal data and criminal records personal data, for one year after the termination of the business relationship, but this is subject to: (a) any minimum statutory or other legal, tax, health and safety, reporting or accounting requirements for particular data or records, and (b) the retention of some types of personal data for up to six years to protect against legal risk, e.g. if they could be relevant to a possible legal claim in a County Court or High Court.

Overall, this means that we will "thin" the file of personal data that we hold on clients, customers and suppliers one year after the termination of the business relationship, so that we only continue to retain for a longer period what is strictly necessary.

Integrity and confidentiality

Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Company takes the security of personal data seriously and we have implemented and maintain safeguards which are appropriate to the size and scope of our business, the amount of personal data that we hold and any identified risks. This includes encryption and pseudonymisation of personal data where appropriate. We have also taken steps to ensure the ongoing confidentiality, integrity, availability and resilience of our processing systems and services and to ensure that, in the event of a physical or technical incident, availability and access to personal data can be restored in a timely manner. We regularly test and evaluate the effectiveness of our technical and organisational safeguards to ensure the security of our processing activities.

in order to properly perform their job duties and responsibilities, have access to these files. Files will not be removed from their normal place of storage without good reason. Personal data stored on removable storage media must be kept in locked filing cabinets or locked drawers and cupboards when not in use by authorised members of staff. Personal data held in electronic format will be stored confidentially by means of password protection, encryption or pseudonymisation, and again only authorised members of staff have access to those data.

The Company has network backup procedures in place to ensure that personal data held in electronic format cannot be accidentally lost, destroyed or damaged. Personal data must not be stored on local computer drives or on personal devices.

The data protection legislation requires the Company to notify any personal data breach to the Information Commissioner's Office within 72 hours after becoming aware of the breach and, where there is a high risk to the rights and freedoms of data subjects, to the data subject themselves. A personal data breach is any breach of security which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed and includes any act or omission that compromises the confidentiality, integrity or availability of personal data or the safeguards that we, or our third-party service providers, have put in place to protect them. The Company has procedures in place to deal with any suspected personal data breach and you are required to comply with these. If you know or suspect that a personal data breach has occurred, you must immediately contact our data compliance manager, retain any evidence you have in relation to the breach and follow the Company's data breach policy and response plan.

Your rights to access personal data

Under the data protection legislation, data subjects have the right, on

request, to obtain a copy of the personal data that the Company holds about them by making a written data subject access request (DSAR). This allows the data subject to check that we are lawfully processing their personal data.