

**GDPR DATA PROTECTION POLICY**

**GDPR Norms:**

The General Data Protection Regulation (GDPR) is an EU legislature that objects to giving the citizens of the EU better power and authority over their data. Under this by-law, organizations that handle statistics of EU citizens will have to obey data and privacy instructions.

One of the key necessities according to the GDPR is changes to the Privacy Policy and the same has been accepted and updated by L2B Media to reflect GDPR requirements. We also abide by its key law i.e. to keep EU citizens informed of how industries gather, use, share, protect and process their personal data.

**Transparency to Accommodate GDPR**

To strongly and strictly abide by GDPR, we ensure that we follow the principle of transparency that requires all types of information to be precise, easily available when required, easy to read and should also be clear and written in understandable language. Further, illustrations and images are also to be used to make it clear and better to understand. This information should also be made available at appropriate and easy-to-access sources.

**GDPR General Data Protection Regulation and Compliance**

L2B Media needs to collect and utilize certain information about persons.

These can include suppliers, customers, employees, business contracts and other people the group have a connection with or may need to contact.

The GDPR policy describes how this personal data must meet the company’s data protection standards and be collected, handled and stored to and to comply with the law.

The GDPR policy ensures L2B Media.

* Complies with the data protection regulation and abide by good practices
* Shields the privileges of staff, clienteles and associates
* Is open to how it supplies and procedures individuals data
* Defends itself from the dangers of a data breach.

**Data Protection Laws**

The Data Protection Act 1998 defines how the organization must procure, handle and store personal information to sustain with GDPR.

These instructions apply regardless of whether data is stored electronically, on paper or on other materials.

To obey the law, personal information must be taken and used fairly, stored safely and not disclosed unlawfully.

The GDPR act is underpinned by eight important principals. These say that personal data must:

* Be treated honestly and legally
* Begotten only for precise, legal purposesBe satisfactory, pertinent and not extreme
* Be correct and kept in accordance with the norms
* Not be held for any further than needed
* Shielded in agreement with the privileges of the data subject
* Be protected in suitable ways
* Not be shifted outside the European Economic Area (EEA), unless that country or territory also safeguards an acceptable level of safety.

**People, Risks and Responsibility as per GDPR**

The GDPR policy applies to:

* The head office of L2B Media
* All branches of L2B Media
* All staff and volunteers of L2B Media
* All contractors, suppliers and other people working on behalf of L2B Media

GDPR also applies to all data that the business holds relating to recognizable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

* Names of persons
* Residential addresses
* Email addresses
* Telephone numbers
* …plus any other information relating to persons

**Data Protection Risks as per GDPR**

GDPR policy helps to guard L2B Media from some very real data safety risks, including:

* **Breaches of confidentiality.**

For instance, the information being given out inappropriately.

* **Failing to offer choice.**

For instance, all persons should be free to choose how the corporation uses data connecting to them.

* **Reputational**

For instance, the company could suffer if hackers effectively gained access to complex data.

**Responsibility as per GDPR**

Everyone who works for or with L2B Media has some accountability for ensuring data is collected, kept and handled appropriately, particularly when it comes to GDPR.

Each team that handles individual data must ensure that it is handled and treated in line with the GDPR policy and data protection principles.

However, these people have key areas of responsibility:

The board of directors is ultimately accountable for ensuring that L2B Media meets its legal obligations.

* The Data Protection Officer is responsible for:
* Keeping the board efficient on data protection responsibilities, dangers and matters.
* Reviewing all data protection measures and related strategies, in line with an agreed timetable.
* Positioning data protection training and information for the people covered by this policy. Taking and answering data protection questions from staff and anyone else covered by this policy.
* Taking and answering data protection questions from staff and anyone else covered by this policy.
* Dealing with wishes from individuals to see what L2B Media holds about them [subject access requests].
* Examining and approving any contracts or agreements with third parties that may handle the company’s sensitive data.
* The IT Manageris responsible for:
* Ensuring all organizations, facilities and equipment used for storing data meet acceptable security standards.
* Performing timely checks and scans to ensure security hardware and software is functioning adequately.
* Assessing any third-party services the company is considering using to store or process data. For instance, cloud computing services.
* The Marketing Manager is responsible for:
* Approving any data protection declarations connected to communications such as communications and letters.
* Addressing any data protection questions from press or media outlets like newspapers.
* Where critical, working with other staff to make sure marketing initiatives stick by data protection principles.

**General Staff Guidelines for GDPR**

* The only people able to access data enclosed by this policy should be those who need it for their work.
* Data should not be shared amongst people informally. When access to private information is required, employees can demand it from their line managers.
* L2B Media will provide training to all workers to help them understand their errands when taking data.
* Employees should keep all data safe, by taking sensible protection and following the guidelines below.
* In particular, strong passwords must be used and they should never be made public.
* Personal data should not be disclosed to unlawful people, either within the company or externally.
* Data should be regularly studied and reorganized if it is found to be out of date. If no longer obligatory, it should be erased and disposed of.
* Employees should appeal for help from their line manager or the data protection officer if they are not sure about any feature of data protection.

**Data Storage According to GDPR**

These rules symbolize how and where data should be safely kept and are also laid down as per GDPR. Queries about storing data safely can be directed to the IT manager or data controller.

When data is stored on paper, it should be kept in a protected place where illegal people cannot see it.

These rules also apply to information that is usually kept electronically but has been published for some reason:

* When not required, the paper or files should be kept in a protected drawer or filing cupboard.
* Workers should make sure paper and printouts are not left where unofficial people could see them, like on a printer.
* Data copies should be shredded and disposed of firmly when no longer required.
* When data is stored automatically, it must be protected from unlawful access, accidental removal and malicious hacking attempts:
* Data should be sheltered by strong passwords that are changed frequently and never shared among workers.
* If data is kept on detachable media (like a CD or DVD), these should be kept locked away safely when not being used.
* Data should only be stored on selected drives and servers, and should only be uploaded to support cloud computing services.
* Servers containing individual data should be sited in a secure site, away from general office spaces.
* Data should be backed up regularly. Those backups should be tested frequently, in line with the company’s standard backup procedures.
* Data should never be saved straight to laptops or other mobile devices like tablets, iPad or smartphones.
* All servers and systems containing data should be protected by permitted security software and a firewall.

 **Data Use as Per the GDPR Norms**

Privately held data is of no worth to l2b Media unless the corporation can make use of it. However, it is when private data is improved and utilized that it can be at the utmost risk of damage, exploitation or stealing:

* When working with personal data, employees should make sure that the screens of their computers are always protected when left unattended.
* Private data should not be shared informally. In particular, it should never be sent by email, as this form of messages is not secure.
* Data must be encoded before being shifted electronically. The IT manager can demonstrate how to send data to official external contacts.
* Private data should never be moved outside of the European Economic Area.
* Employees should not save duplicates of personal data to their own systems. Continuously access and keep up-to-date the main copy of any information.

**Data Accuracy for GDPR Compliance**

The law requires L2B Media to take rational steps to ensure data is kept correct and up to date when it comes to GDPR.

The more significant it is that the personal data is accurate, the greater the effort L2B Media should put into safeguarding its accuracy.

It is the responsibility of all employees who work with data to take judicious steps to safeguard it is kept as accurate and up to date as possible.

* Data will be held in a few places as needed. Staff should not create any pointless additional data sets.
* Workers should take every chance to make sure that the data is updated. For instance, by authorizing a customer’s details when they call.
* L2B Media will make it easy for data subjects to update the data L2B Media holds about them. For instance, via the company website [www.l2bmedia.com]
* Data should be reorganized as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be eliminated from the database.
* It is the marketing manager’s duty to ensure marketing databases are checked against company-suppression files every six months.

**Subject Access Requests In Terms of GDPR**

All individuals who are the subject of individual data held by L2B Media are entitled to:

* Ask what evidence the company holds about them and why.
* Ask how to gain admission to it.
* Be knowledgeable about how to keep it up to date.
* Be knowledgeable about how the company is meeting its data protection responsibilities.

If any person contacts the company requesting for this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at info@l2bmedia.com the data supervisor can supply a standard request form, although other persons do not have to use this. Entities will be charged £10 per topic access request. The data controller will aim to deliver the relevant data within 14 days.

The data controller will always confirm the individuality of anyone making a subject access request before passing over any information.

**Disclosing Data for Other Reasons**

In certain conditions, GDPR allows personal data to be disclosed to law enforcement agencies without the agreement of the data subject.

Under these circumstances, L2B Media will disclose demanded data. However, the data controller will ensure the request is genuine, seeking assistance from the board and from the company’s legal guide where essential.

**Providing Information for GDPR**

L2B Media aims to ensure that persons are conscious that their data is being handled and that they understand:

* How the data is being used
* How to exercise their privileges

To these ends, the company has a confidentiality statement, setting out how data connecting to individuals is used by the company.

**Data Protection Officers**

The Data Protection Officer at L2B Media is accountable for assisting the business with internal compliance and also notifies and advises the company about its data protection obligations provides important references regarding any Data Protection Impact Assessments and acts as a go-to person for data subjects.

**Important Information of L2B Media Being GDPR-Friendly**

L2B Media’s privacy policy document is structured for use in relation websites which gather and processes various kinds of private information. Our sole purpose here is to help website operators meet their requirements under the GDPR norms.

The GDPR policy covers, amongst other things, the following matters:

* Several groups of personal information that has been composed and stored by the website;
* information about cookies used by the site;
* facts of how private information is used;
* certification of the legal bases for dispensation personal data;
* details of precise situations in which personal data may be disclosed to third parties;
* information about the transmission of personal data; and
* information about data holding guidelines.

Those on the L2B Media website and all its clients are requested to kindly read the notes related with the privacy policy very judiciously. In relation to cookies, our privacy policy also states that the users’ agreement is required to take and store cookies.

**GDPR Rights to Safeguard Our Clients**

If you or any of your industries deal with L2B Media, we make sure you have all the below-mentioned rights in accordance with GDPR:

* **The right of Admittance:** When it comes to L2B Media, every client or member has the right to obtain information from us concerning whether or not personal data is being used, along with where and how the utilization is happening, making sure people have the right to appeal and get access to their personal data.
* **Right to Alteration:** Clients have the right to attain from us the alteration of imprecise personal data and also the right to provide extra personal data to complete any partially-provided private data.
* **Right to Removal:** In certain cases, clients have the right to get from us the elimination of their personal data, for whatsoever reason.
* **Right to Constraint of Usage:** Clients definitely have the right to obtain from us limit of data use and processing that is appropriate for a certain period and/or for crucial situations.
* **Right to Portability of Data:** Clients have the right to obtain from us in a prepared format their personal data and also have the right to convey such personal data to another organizer.
* **Right to Object:** In certain cases, clients have the right to object to the dispensation of their personal data, including with regards to profiling. They also have the right to object any further processing of any private data, such as data that has been gathered for direct marketing means.
* **Right to Individual Decision-Making:** As per GDPR, clients have the right to not be subject to a choice based solely on automatic processing.
* **Right to Filing Complaints:** One also has complete rights to file grievances with the official data protection authority on the processing of any of their personal data.
* **Right to Compensation of Damages:** In case there is any breach applicable legislation on the processing of personal data, one also has the right to claim recompenses from us for any costs such breach may be caused.