Lancetech Limited

6 Sevenways Parade
Woodford Avenue
Ilford, IG2 6XH UK
www.lancetechltd.com

Policy on Data Security

Meaning and Explanation

Automated Decision-Making (ADM): refers to choices made exclusively by computer programmes (including profiling) that yield legal consequences or substantially impact a person. The GDPR forbids Automated Decision-Making (ADM) unless specific circumstances are satisfied, although it does not ban automatic processing.

Automated Processing: refers to any kind of computerised handling of private information employed to assess certain personal characteristics of an individual, including employment efficiency, financial status, health, unique tastes, objectives, reliability, behaviour, setting, or activities. Profiling exemplifies mechanised processing.

Company Name: refers to Lancetech Ltd.

Corporate Staff: means every staff member, staff, subcontractors, agency personnel, professionals, executives, teammates, and etc.

Consent: means permission that is freely offered, explicit, and up to date, as well as an unequivocal expression of the desires of the data subject for the project. The Data Subject gives their explicit consent to the processing of their personal data by making a statement or taking an affirmative action.

Data Controller: means the individual or entity that determines the time, justification, and manner of processing personal data. Individuals or organisations. tasked with the responsibility of establishing policies and processes that are in accordance with the General Data Protection Regulation (GDPR). It is the responsibility of Lancetech Ltd. to act as the data controller for any and all personal information that belongs to its employees and is used for business purposes inside the company.

Data Subject: means a live, named, or identifiable individual whose personal information is maintained and who is considered to be a citizen. The individuals who act as data subjects may be citizens or residents of any nation, and they may be entitled to certain legal rights in connection with their personal data.

Data Privacy Impact Assessment (DPIA): means in order to detect and reduce the risks connected with data processing activities, evaluations and instruments were put into place. Data Privacy Impact Assessments (DPIAs) should be carried out for any substantial system or business improvements that include the processing of personal data, and they can be a component of the Privacy by Design initiative.

Data Protection Officer (DPO): means under the General Data Protection Regulation (GDPR), the person who is needed to be assigned in certain instances. In the absence of a statutory data protection officer (DPO), this phrase refers to a data protection manager or another voluntary appointment of a DPO, or the data privacy team of the organisation that is responsible for ensuring compliance with data protection regulations.

EEA: means together with Iceland, Liechtenstein, and Norway, the 28 nations that make up the European Union.

Explicit Consent: means a statement that is both explicit and specific (i.e., not merely an action) is necessary for assent.

General Data Protection Regulation (GDPR): Protecting individuals' personal information is the purpose of the General Data Protection Regulation (EU) 2016/679, which is a legal framework.

Personal Data: "personal data" refers to any information about an individual that can be used to identify them, whether that identification is based on the data alone or on other identifiers that we have or can get in order to identify them. On the other hand, personal data does not include information that does not identify a specific individual or that has had their identity erased entirely. Personal data includes both sensitive data and data that has been pseudonymized. Factual information (such as a person's name, email address, location, or date of birth) and objective evaluations of their activities or behaviours can both make up personal data, or both can be combined.

Personal Data Breach: constitutes a potential violation of privacy if any action or failure to act compromises the security of personal data and the measures implemented to protect it, whether those measures be mechanical, managerial, or organisational. Data breaches can happen when critical information is either obtained, released, lost, or accessed without authorisation.

Privacy by Design: Implementing the essential organisational and technological steps to guarantee compliance with the General Data Protection Regulation (GDPR).

Privacy Guidelines: means the privacy and GDPR-related guidelines that the Company has developed in order to assist in the interpretation and implementation of this Data Protection Policy and any other policies that are linked with it.

Disclaimers of Privacy (also known as Fair Processing Notices) or Policies of Privacy: signifies that whenever the Company gathers data pertaining to Data Subjects, distinct notifications are sent out detailing the details that those who provide data may be informed of by the Company. These notifications can be comprehensive privacy statements that apply to a specific group of individuals (such as website policies or employee privacy notices) or they can be separate, one-time privacy statements that address Processing for a specific purpose.

Processing or Process: denotes a procedure that makes use of individual data. Any process or set of activities performed on data, including organising, modifying, retrieving, using, revealing, deleting, or destroying it, is part of data management. So is data collecting, documentation, or preservation. One aspect of data processing is the communication or transfer of personally identifiable information to other parties.

Pseudonymization or Pseudonymized: signifies substituting information that directly or indirectly identifies a person with one or more fake identities or pseudonyms, ensuring that

the data's intended recipient cannot be identified without additional, independently stored information.

Related Policies: means the policies, operational procedures, or activities of the organisation that are related to this Data Protection Policy and are done with the intention of protecting Personal Information.

Sensitive Personal Data: includes, but is not limited to, a person's racial or ethnic background, political views, religious or similar beliefs, union membership, health status (mental or physical), sexual orientation, history of sexual activity, biometric or genetic information, and details about criminal records and convictions.

Introduction

The purpose of this Data Protection Policy is to outline the manner in which Lancetech Ltd. (hereinafter referred to as "we," "our," "us," and "the Company") handles the Personal Data of our clients, vendors, employees, and other third parties.

Every piece of personal information that our company collects or stores, whether it's from current or past employees, contractors, clients, shareholders, website visitors, or any other Data Subject, is subject to our Data Protection Policy. Every member of the Company's staff (referred to as "you" or "your") is required to comply with this Data Protection Policy. In order to comply with this Data Protection Policy, you are needed to read it, understand it, and adhere to it while processing Personal Data on our behalf. Additionally, you are obliged to engage in training about the requirements of this policy. When it comes to ensuring that the Company is in conformity with applicable laws, our Data Protection Policy outlines the expectations that we have of you. There is no exception to the need that this Data Protection Policy be followed. To assist you in reading and complying to our Data Protection Policy, related policies and privacy guidelines are available for your perusal. It is required that all Related Policies and Privacy Guidelines be adhered to at all appropriate times. It is possible that disciplinary actions will be taken in response to any infringement of our Data Protection Policy.
No third party, client, or authority may access this Data Protection Policy, Related Policies, or Privacy Guidelines without the prior approval of the Data Protection Officer (DPO). This is because the documentation is considered confidential.

Scope

We are aware that the organization's ability to handle personal data in a manner that is both appropriate and lawful will foster trust in the organisation and make it easier to conduct successful business operations. Maintaining the privacy and integrity of individuals' personal information is our top priority, and we will never waver in this regard. Fines of up to 4% of total worldwide annual revenue (or 20 million Euros, or about £18 million) might be levied against the Company if it does not adhere to the General Data Protection Regulation (GDPR). The type of violation determines the penalty. Ensuring that all workers comply with this Data Protection Policy is the responsibility of every department, division, and supervisor in the

organisation. A combination of suitable rules, procedures, controls, and training may guarantee adherence to this policy.

The responsibility of overseeing the Data Protection Policy and, when applicable, developing accompanying policies and privacy standards falls within the purview of the Data Protection Officer (DPO). Please do not hesitate to get in touch with the Data Protection Officer if you have any questions or issues regarding the implementation of this Data Protection Policy or the General Data Protection Regulation (GDPR), or if you have any reservations regarding the adherence to this policy.

In particular, you are obligated to get in touch with the DPO under the following particular circumstances:

a) Should you be unsure about the legal basis for processing personal data (which may include the legitimate interests of the Company), you should consult the following:
b) In the event that you require consent and/or have a requirement to get explicit consent,
c) In the event that you are required to draft Privacy Notices or Fair Processing Notices,
d) If you have any questions regarding the length of time that the personal data that is being processed will be stored,
e) In the event that you are unsure about the precautions that must be taken to protect personal data,
f) the event that there has been a breach of personal data,
g) if you are unclear about the legal basis for transferring personal data outside of the European Economic Area (EEA), or.
h) if you want assistance in resolving any rights that have been asserted by a customer or client.
i) If you plan to use personal data for purposes other than those for which it was first obtained, or if you perform a significant new or modified processing activity that is likely to warrant a Data Protection Impact Assessment (DPIA), you are required to notify the Privacy Commissioner.
j) If you plan on participating in activities that are associated with automated processing, such as profiling or automated decision-making, you should contact us.
k) If you are interested in receiving advice in conforming to applicable regulations while engaging in direct marketing activities; or
l) in the event that you are looking for advice about contracts or other issues concerning the disclosure of personal data to third parties (including our suppliers), we are here to assist you.

Norms for the Protection of Individual Information

We comply with the guidelines for the Processing of Personal Data established in the GDPR, which mandate that Personal Data must be:

a) Executed in a lawful, equitable, and transparent way (Respect for the law, equity, and openness to information).
b) Stored solely for defined, stated, and justifiable objectives (Purpose Limitation)

c) Data that is sufficient, relevant, and limited to the information that is necessary for the processing of the data (data compression).
d) "Precision" means accurate and, where applicable, up-to-date information; "Storage Limitation" means data is not stored for longer than is strictly required for processing purposes without sacrificing data accuracy.
e) Safeguarded against loss, accidental destruction, or damage, and unauthorised or unlawful processing to guarantee its security (Security, Integrity, and Confidentiality). The right technological and organisational approaches allow us to achieve this.
f) Data Subjects are allowed access to their personal data and are authorised to exercise certain rights with regard to it (Data Subject's Rights and Requests). Without appropriate protections in place, data subjects are not located in a foreign country (Transfer Limitation).

We are accountable for the aforementioned data protection standards, and we are required to demonstrate that we comply to them according to the norms.

Respect for the law, equity, and openness to information

Personal information must be treated in a manner that is lawful, fair, and transparent with regard to the individual whose data is being processed.

It is only permissible to collect, handle, and exchange personal data in a manner that is both fair and legal for the purposes that have been defined. Our actions involving personal data are restricted to specific legitimate objectives as a result of the General Data Protection Regulation (GDPR). The purpose of these limits is to make processing easier while also ensuring that we manage personal data in a fair manner and without having a detrimental impact on the person whose data we are processing.

Certain processing is permitted under the General Data Protection Regulation (GDPR), several of which are described below:

In order to process information, we need the data subject's consent, it's essential to fulfil a contract with the data subject, protect the data subject's vital interests, or pursue our legitimate interests (as long as they don't harm the data subjects' interests or basic rights and freedoms). The relevant Privacy Notices or Fair Processing Notices must specify the reasons why we treat Personal Data in order to pursue legitimate interests.

Consent

Data Controllers are required by the General Data Protection Regulation (GDPR) to get consent before processing any personal data. When an individual makes a clear declaration or takes an affirmative action, they are giving their consent for the processing of their personal data.

Because clear action is required for consent, pre-checked boxes, or doing nothing are frequently not sufficient. The provision of consent must be clearly distinguished from any other matters addressed in the agreement.

At any moment, data subjects are able to revoke their consent to processing, and we must promptly recognise this revoked consent. If you intend to use the data for anything unrelated to what was disclosed when the data subject originally gave their approval, you will need to get their consent again. Explicit Consent is typically required in cases where no other legal basis for processing exists, particularly when dealing with automated decision-making, cross-border data transfers, and the processing of sensitive personal data. For the most part, we will not need Explicit Consent to Process Sensitive Data since we rely on other legal grounds. A Fair Processing Notice must be given to the Data Subject in order to get Explicit Consent where it is essential.

By keeping track of all Consents and documenting those that have been acquired, the Company may ensure compliance with Consent rules.

Data Subject Notification for Transparency

Regardless of where the data originated from, the General Data Protection Regulation (GDPR) requires Data Controllers to provide Data Subjects with complete and accurate information.
To make sure a Data Subject can easily understand them, the appropriate Privacy Notices or Fair Processing Notices must be brief, transparent, understandable, easily available, and written in plain and simple language. When we directly collect personal information from individuals for HR or employment-related purposes, we must provide them with all the information required by the GDPR. At the time the Data Subject initially provides the Personal Data, we provide them with a Fair Processing Notice that explains how and why we will use, process, disclose, protect, and keep their data. This notice also reveals the identities of the Data Controller and DPO.

If the Data Subject's Personal Information was acquired indirectly, for example via a third party or a publicly accessible source, you are obligated to inform them of all necessary details under the General Data Protection Regulation (GDPR) without undue delay following data collection or reception. It is critical to ensure that the third party collected the Personal Data in a way that complies with the GDPR and allows us to process it as intended. When drafting Privacy Notices or Fair Processing Notices, be sure to follow the company's procedures.

Restrictions on Use

Only for clear, legitimate, and purposeful purposes may personal information be collected. Processing it in a way that undermines their goals is strictly forbidden.

The Data Subject must be informed of any changes to the original purpose of their personal data and given their consent before the data can be used for new, different, or incompatible purposes.

Data Minimisation

Personal information must be sufficient, relevant, and limited to what is strictly required in order for it to be processed. Only when processing personal data is absolutely necessary to

carry out your job duties is it acceptable. Processing personal data for purposes unconnected to your job description is strictly prohibited. Keep in mind that you should only acquire Personal Data that is absolutely required to carry out your job duties. Verify that the data acquired is sufficient and applicable for the planned purposes. It is critical to delete or de-identify Personal Data once it is no longer needed for specific reasons, in accordance with the Company's data retention policy.

Accuracy

All personally identifiable information must be accurate and, if necessary, kept up-to-date. When it's wrong, it has to be fixed or eliminated right away.

You are responsible for ensuring that the Personal Data we collect, use, and store is accurate, complete, up-to-date, and relevant to its intended use. Checking the accuracy of any Personal Data at the point of collection and on a regular basis afterwards is vital. It is imperative that all reasonable efforts are made to repair or erase inaccurate or out-of-date Personal Data.

Restriction on Storage Space

No longer than is strictly necessary for processing purposes should personally identifiable information be kept in an identifiable format. After the initial legitimate business reason of obtaining the data (such as compliance with accounting, reporting, or regulatory requirements) has passed, personal data must not be kept in a way that might be used to identify the Data Subject. Unless a shorter retention period is mandated by law, the Company will establish retention policies and procedures to erase Personal Data after a reasonable amount of time has passed that is appropriate for its intended purposes. In compliance with the relevant records retention schedules and policies of the Company, you must ensure that any Personal Data that is no longer needed is deleted or removed from our systems. Requiring third parties to remove such material may be part of this process in some instances. The relevant Privacy Notice or Fair Processing Notice shall notify Data Subjects of the data retention duration and the criteria used to calculate it.

Protecting Data, Honesty, and Secrecy

Data Security for Individuals

An appropriate level of technical and organisational protection is required to prevent the loss, misuse, alteration, or destruction of personal data, as well as its unauthorised or unlawful processing.

We shall implement measures, such utilising encryption and pseudonymization where necessary, that are commensurate with our size, scope, operations, available resources, quantity of personal data we own or manage for others, and the recognised risks. Regular evaluation and testing of these methods will ensure the safety of our personal data processing. It is on you to keep safe any personally identifiable information that we may have in our possession. Implementing suitable and efficient security measures can avoid the accidental loss, destruction, or unauthorised or unlawful handling of personal data. Adherence to

relevant laws and regulations is essential for protecting Sensitive Personal Data against accidental or unlawful destruction, modification, or disclosure.

From the moment of collection to its eventual deletion, all measures taken to protect individuals' personal information must be strictly adhered to. Only third-party service providers that agree to follow the necessary protocols and take the necessary measures will their personal data be transmitted.
Preserving the privacy, accuracy, and accessibility of personally identifiable information (PII) is of the utmost importance, as outlined below:

a) The term "confidentiality" refers to the restriction of access to Personal Data to those who have a "legitimate need to know" and the appropriate permission.
b) For personal data to be considered "integrated," it must be accurate and suitable for its designated use.
c) Availability signifies that permitted individuals can access Personal Data when required for sanctioned reasons.

We take administrative, physical, and technical safeguards to secure Personal Data in line with the GDPR and other applicable regulations. You must comply to these precautions and not attempt to bypass them.

Complaining about a Security Breach

Data Controllers are required under the GDPR to notify the appropriate authorities and, in certain cases, the Data Subject, in the event of a Personal Data Breach. If we become aware of a possible breach of personally identifiable information, we shall follow our procedures and notify the appropriate authorities as soon as possible.

Stay out of any enquiry into a personal data breach if you know about it or have suspicions about it. Please inform the Data Protection Officer or the Finance Director, as soon as possible, or the designated team responsible for handling personal data breaches. It is imperative that all records related to the possible breach of personal data be kept.

The Boundaries of Transfer

To keep the data protection standards offered to individuals under the GDPR intact, the regulation restricts data transfers to countries outside the EEA. The transmission, sending, viewing, or access of personal data inside or to a foreign country is known as a cross-border transfer.

One of the following conditions must be satisfied before personal data can be transferred beyond the EEA:

a) The data recipient nation is deemed by the European Commission to provide sufficient data subjects' right to privacy and freedom of choice;
b) Appropriate safeguards, such as binding corporate rules (BCR), EU-approved standard contractual terms, an endorsed code of conduct, or a certification

procedure, are implemented; the Data Protection Officer (DPO) can provide a copy of these documents.

c) Following a thorough explanation of the risks involved, the data subject has provided their express approval for the planned transfer.
d) Transferring the data is essential for one of the other reasons specified in the General Data Protection Regulation (GDPR). These include fulfilling a contract we have with the Data Subject, considering public interest, establishing, exercising, or defending legal claims, safeguarding the Data Subject's vital interests when they cannot give Consent because of physical or legal limitations, or, in certain instances, for our legitimate interests.

Transfers of data across international borders must adhere to the standards set out by the Company.

Requests and Rights of Data Subjects

Individuals have control over how their personal information is handled. For example, you have the right to: withdraw your consent to processing at any time;

a) learn the details of the Data Controller's processing operations;
b) request access to the personal information that we have on file for them;
c) outright forbid us from using their personal information for commercial reasons;
d) ask for the removal of personally identifiable information (PII) when it is no longer needed for the purposes it was collected or processed, rectify erroneous or incomplete data, or request its erasure altogether;
e) limit operations under particular circumstances;
f) challenge processing that is supported by our rightful interests or the greater good;
g) ask for a copy of the document that governs the transfer of personal data outside the European Economic Area;
h) reject decisions made only by ADM, which includes profiling;
i) avoid Data Subject or third party discomfort or injury through Processing;
j) be made aware of a potential threat to their rights and freedoms posed by a Personal Data Breach;
k) file a formal grievance with the appropriate supervisory body; and
l) request a third party to send their personal data to them in a generally used, machine-readable format under certain circumstances.

Never give out your personal information to a third party without their express permission, and always verify their identification if you receive a request for personal data in response to one of the rights listed above. You have an obligation to notify your supervisor or the Data Protection Officer (DPO) without delay upon receiving a data subject request.

Accountability

In order to ensure compliance with data protection regulations, the Data Controller must efficiently implement appropriate organisational and technological safeguards. Compliance with data protection requirements is the responsibility of the Data Controller, who must be able to provide evidence of this.

The Company must establish sufficient resources and controls to ensure and document GDPR compliance, which includes:

a) finding and appointing an appropriate executive to oversee data privacy and a trained Data Protection Officer as required;
b) using this Data Protection Policy and other internal documents to safeguard personal information, such as Privacy Guidelines, Notices to Users, and Fair Processing Notices;
c) on a regular basis, educating employees on topics such as the General Data Protection Regulation (GDPR), this policy, any relevant rules or privacy standards, data protection concerns (including problems like personal data breaches, data subject rights, consent, legal basis, and data protection impact assessments), and more.
d) In order to ensure compliance, the company must keep track of when employees have received training and conduct regular reviews and audits of the privacy protections in place. The results of these reviews and audits should be used to demonstrate how the company is working to improve compliance.

Record Keeping

All data processing actions must be meticulously documented in accordance with the General Data Protection Regulation (GDPR).
The accuracy and completeness of the records pertaining to our Processing, including those pertaining to the consents of data subjects and the methods used to obtain them, must be maintained in accordance with the standards set forth by the company.

Data subjects' categories, processing activities, purposes, third-party recipients, storage locations, transfers, retention period, and security measures should all be clearly described in the records. The names and contact information of the data controller and data protection officer should also be included. The development of data maps that incorporate the aforementioned information and pertinent data flows is necessary for the generation of such records.

Training and Audit
To ensure compliance with data privacy regulations, it is necessary that all Company Personnel undergo adequate training. To keep in line with regulations, we need to review our processes and systems often.

You must finish all mandatory data privacy training and make sure your team does the same, following the company's training regulations. In order to ensure that all systems and processes under your control are following this Data Protection Policy and that you are providing enough supervision, it is crucial that you conduct regular assessments.

Privacy by Design and Data Protection Impact Assessment (DPIA)

To ensure compliance with data privacy regulations, we must use Privacy by Design procedures when handling personal data. This includes using appropriate organisational and technical methods, such pseudonymization. All programmes, systems, and processes that deal with personal data must undergo a thorough evaluation to determine whether Privacy by Design measures may be implemented. This evaluation must take into account a variety of factors, including the available technology, the expense of implementation, the goals, context, and form of processing, and the dangers to data subjects' rights and freedoms that may result from processing, the severity and probability of which can vary.

Regarding Processing that poses a significant risk, data controllers are likewise need to do DPIAs.

Every time a major system or business change is about to be implemented that may affect the processing of personal data, a Data Protection Impact Assessment (DPIA) needs to be conducted and the results should be shared with the Data Protection Officer (DPO). This includes:

a) incorporating newly developed or improved technological systems, programmes, or procedures;
b) computing, which encompasses automated decision-making (ADM), profiling, and automated processing;
c) thorough handling of Private Information; and,
d) massive, organised tracking of open spaces.

Included in a DPIA are:

a) Data Processing, including its purposes and the Data Controller's (if any) legitimate interests
b) a review of the Processing's relevance and appropriateness in light of its intended use;
c) an examination of the potential dangers to persons; and
d) proof of compliance and the risk mitigation techniques that were put into place.

There can be no exceptions to the Company's DPIA and Privacy by Design regulations.

Direct Marketing

The promotion we do for our clients and consumers must be compliant with various privacy laws and regulations.

Data Subjects must provide their approval before any electronic direct marketing, such as email, SMS, or automated calls, can take place. If a business has the recipient's contact information from a prior transaction, is advertising similar products or services, and gave the recipient the opportunity to decline marketing communications both when they were collecting their data and in all subsequent correspondence, then the recipient can receive marketing messages via text or email (with the exception of existing customers, where this is called "soft opt-in"). It must be shown clearly and legibly so that the Data Subject can

quickly find it among other information, however they do have the right to object to direct marketing.

Data subjects have the right to swiftly object to direct marketing. Quick data suppression is required in the event that a customer wishes to opt out. Keeping enough data to ensure the future recognition of marketing decisions is what suppression is all about.

In all matters pertaining to direct marketing to clients, the Company's orders must be followed.

Disclosure of Private Information

The sharing of personally identifiable information with other parties is often prohibited in the absence of appropriate protections and agreements. To ensure compliance with relevant cross-border transfer regulations and to prevent unauthorised access, we will restrict access to your personal data to those employees, agents, or representatives of our group, which includes subsidiaries and the ultimate holding company with its subsidiaries, who have a legitimate need to know it for their job.

Only in the following situations will third parties, including service providers, be granted access to personal data:

a) they need the data to complete the service they agreed to;
b) the sharing follows the guidelines laid out in the Privacy Notice that was given to the Data Subject, and if needed, they have obtained the Data Subject's consent;
c) the third party has promised to follow all the rules when it comes to data security and has put in place sufficient safeguards;
d) the transfer complies with all applicable regulations regarding international data transfers; and
e) a legally binding agreement with GDPR-compliant third-party provisions has been obtained.

Everyone must follow the company's rules when it comes to sharing information with outside parties.

Updates to this Privacy Statement

We may, at any moment and without notice to you, change this Data Protection Policy.

No applicable data privacy laws or regulations of the countries in which the Company conducts business shall be superseded by this Data Protection Policy. The Data Protection Officer (DPO) can provide you with any localised versions of this policy that may be available upon request.

Contact Information
Enquiries, remarks, and requests pertaining to this privacy policy are encouraged and should be directed to our response administrator at Lancetech Limited, 6 Sevenways Parade, Woodford Avenue, Ilford, IG2 6XH, or by email using the online form on our website.