Privacy Notice

1. Introduction

This privacy notice is a public document, which tells you what to expect when Sensical Services Ltd ("Sensical") processes your personal data and the lawful basis for all processing we have.

We explain what choices and rights you have with respect the data we MAY collect from you. We take into consideration Information Commissioner Office's (ICO) guidelines and best practices as well as all the additional elements of General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

This privacy notice is consistent with our Information Commissioner Office (ICO) Public Registration (Certificate ZA372483) and our Personal Data Protection Policy, which governs the use and storage of the personal data we collect.

2. What we need and what is the purpose of processing

We process personal information about our stakeholders including clients, professional advisers and consultants and our employees. Each one of the following processing activities describes on one hand the types of personal data that we MAY collect from you and on the other hand, the specific lawful purpose we have. Note that Sensical is a data controller of the personal data that you, as a data subject, provide to us.

Company Staff administration is the purpose of processing:

- Note that the source the personal data originates from is a form "New Employee CheckList" filled by you as data subject.
- We MAY collect from our employees:
    - For compliance with legal obligations, we need to collect the following personal data types from our employees (e.g. HMRC obligations - See https://www.gov.uk/paye-for-employers/keeping-records.).
        - Staff contact details. See notes (1) and (2).
        - Staff emergency contacts details.
        - PAYE and payroll data (e.g. name, bank details, address, date of birth, national insurance number, pension arrangements and salary).
        - Right to work data (Visa, Proof of identity etc.).
        - Health data such as Maternity/Paternity Leave or Sickness Absence data to facilitate the payment of statutory sick pay, etc.
    - For contractual necessity, because you have applied for a job vacancy where our customers require a background screening, before entering into a contract with you.
        - Employment screening data, should you have given us written consent, within the constraints of local laws. Examples of background checks MAY include previous employment history, when applicable criminal records, credit history, and reference checks. Note that checks are authorised by law, for example, roles involving work with vulnerable adults or children where a Disclosure and Barring Service check is required. See https://www.gov.uk/employers-checks-job-applicants

- On the basis that you have consented to such processing:
  - Biometrics where used solely for ID purposes (e.g. secure access control to your company laptop, logical systems or physical premises).
  - Copy of CV (e.g. name, contact details, employment and education history).
  - Notes of interviews.

Contact request administration is the purpose of processing:

- Source the personal data originates from is information provided by you directly (e.g. Online enquiry or email).
- We MAY collect:
  - Under a contract or only because you have asked us to do something before entering into a contract (e.g. provide a quote, responding to your requests, comments and questions)
    - E-mail - Note that when you send us an email (e.g. support@sensical.net) we collect your business contact details and email address.
    - Contact details (Name, corporate E-mail address, Job Title, Company, telephone).
  - Based on legitimate interest to help improve our efficiency and effectiveness dealing with your requests.
    - Helpline Calling ID information. - Note that when you call our helpline we collect the CID.
    - Social media ID - Note that if you have a social media user account and you send us a private or direct message via our social media account (e.g. Twitter or LinkedIn), we may collect your social media identifier and the message, which will be stored in our corporate social media account.

Customer/Suppliers orders, shipping goods or services delivering is the purpose of processing:

- Source the personal data originates from is information provided as part of a contract.
- We MAY collect:
  - Personal data types collected in order to enter into or perform a contract with you being the point of contact of your organization (e.g. order / goods shipping or services delivering).
    - Contacts details (e.g. your name, your corporate e-mail address, job title, company, telephone).
    - Financial details of your order (e.g. order number, payment, billing details).
    - Shipping/Delivery details.
- You may decide that under our written contract, additional personal data to be processed by us, provided that you have a valid lawful basis. Under GDPR then a Supplier Data Processor Agreement (DPA) should be in place describing your instructions on how we should process personal data on behalf of you, the purpose of processing you require, a list of personal data types in the scope of our processing activities, security controls required and approved sub-processors (e.g. cloud services).

- Additional data we MAY collect, when delivering IT services, under a Data Processor Agreement, where Sensical Services acts as a data processor, appointed by you, and then you acts as a data controller:
    - The full document is agreed between both parts depending on the type of service you are using (Network Services, Cloud Services, Communications and Security) e.g.:
        - Backup of your data or an archive including personal data and "business" email.
        - Infrastructure as a Service - IaaS - (CPUs, Memory, Backup, Storage, Network, Virtual Machines) processing personal data (e.g. endpoint IP Addresses).
        - Platform as a service - PaaS - Management (Windows Server, Email Server, Directory Server) processing personal data (e.g. users names and email addresses).
        - Software as a service - SaaS - Management (Website, Cloud Applications, Email, AD, Desktop) processing personal data (e.g. Visitor IP Address, online identifiers).
        - IT Service Desk service and Remote access tools that provide screen transfer processing personal data (e.g. users names and email addresses, endpoint IP addresses, device identifiers).
        - Security Audits (Cyber Essentials, PCI-DSS, GDPR) processing personal data (e.g. users names and email addresses, endpoint IP addresses, device identifiers, access credentials).
        - Infrastructure vulnerability assessment and penetration testing processing personal data (e.g. user names and email addresses, endpoint IP addresses, online identifiers).
        - Logs and audit records administration and monitoring processing personal data (e.g. user names and email addresses, endpoint IP addresses, online identifiers).

IT infrastructure performance and security incidents handling is the purpose of processing.

- We need personal data types collected under relevant legitimate interests.
- Source the personal data originates from is predominantly our IT & Security systems (e.g. firewalls, routers etc.) collecting IP addresses from visitors accessing our IT Infrastructure.
- Alternative source of data can be a paper or digital visitor book filled by the data subject when visiting the physical premises of the company.
- We MAY collect:
    - Device-specific information (attributes such as operating system and device identifiers of the computer, mobile phones or other devices)
    - Physical ID, ID token or digital certificate
    - Biometrics where used solely for ID purposes (e.g. secure access control to our company logical systems or physical premises).
    - Visitor / User IP Addresses
    - Visitor name, date/time entrance and exit as well as person receiving the visit.
    - User account credentials
    - Log information

- Device event information
- Location information
- On-line Identifiers as cookies or similar technologies required to enable core site functionality (Provide secure login, remember your login details, and make sure your website looks consistent) or cookies required to measure and improve performance.
- No advertising cookies are processed and users are not tracked.

Legitimate B2B marketing communication purpose of processing.

- We need personal data types collected under relevant legitimate interests. We balance our legitimate interests against your individual's interests, rights and freedoms.
- Note that we have conducted a Legitimate Interests Assessment ("LIA") and kept a record of it, to ensure that we can justify our decision.
- Source the personal data originates from is information provided by you directly (e.g. Online enquiry or email).
- Note that we may process your personal information for carefully considered and specific purposes which are in our interests and enable us to enhance the services we provide, but which we believe also benefit our customers i.e. to contact you sometimes and better understand the kind of services you are interested in.
- We MAY collect:
    - Contacts details (your name, your corporate e-mail address, job title, company and telephone) See note (1) and (2).

Consent based B2B marketing communication is the purpose of processing:

- This processing activity only take places with your explicit consent.
- Note that under GDPR, we will require you a positive opt-in (pre-ticked boxes cannot be used or any other method of default consent).
- Source the personal data originates from is a form filled by you, web user interaction as well as social media interaction via corporate accounts in Twitter and LinkedIn.
- Purpose of processing include a better understanding how people interact with our website. We MAY use a website digital analytics which is GDPR compliant. Analytics is a process or set of measurements that help us to understand the website business performance, to see what visitors are doing on our site, how they interact with it, how we are helping them to accomplish their tasks, understand their behaviour, their preferences, what advertising campaign is performing better, visitor tracking, generate reports about visitors. We may send you marketing messages so you can control whether you receive them.
- Please bear in mind that if you object, you can opt-out, however this may affect our ability to help you to accomplish your tasks efficiently for your benefit (e.g. download a security assessment template of your interest).
- We MAY collect:
    - Contacts details (your name, your corporate e-mail address, job title, company and telephone) See note (1) and (2).
    - Device-specific information (attributes such as operating system and device identifiers of the computer, mobile phones or other devices)

- Visitor/ User IP Addresses
- Social media identifiers (Twitter, LinkedIn)
- Log information
- Device event information
- Location information
- On-line Identifiers as cookies or similar technologies required to enable core site functionality (provide secure login, remember your login details, make sure your website looks consistent) or required to measure and improve performance.
- Advertising cookies are collected. These cookies are used by advertising companies to track users and to serve ads, which are relevant to your interests and allow you to share pages with social networks.

General Notes:

(1) Note that processing special category data which GDPR says is more sensitive (race, ethnic origin, politics, religion, trade union membership, genetics, biometrics where used for ID purposes, health, sex life, sexual orientation) shall be prohibited, unless you have given us explicit consent to the processing of those personal data for one or more specified purposes. (See GDPR Art. 9).

(2) Note that personal data related to criminal convictions and offences if processed by third parties will follow Article 10 GDPR.

3. Why we need it

We process personal information to enable us to provide IT & Security Consultancy and Services to our clients, to maintain our own accounts and records and to support and manage our employees. These are the reasons why we need to process your personal data information:

Company Staff administration:

- If you are an employee from Sensical and as your employer, we need to process personal data to comply with our legal obligation to disclose employee salary details to HMRC (See https://www.gov.uk/paye-for-employers/keeping-records). In addition, the processing is necessary for the establishment, exercise or defence of legal claims. The provision of personal data is a legal obligation and possible consequences of failing to provide personal data is our inability to offer you a position within the company.
- Employers also need to make sure new employees are allow to work in the UK before they hire them. An employer can be fined up to 20,000 GBP if they cannot show evidence that they checked an employee's right to work in the UK (See https://www.gov.uk/employers-checks-job-applicants).
- If you are an employee, we need to verify your identity before providing you a physical ID to have secure access control to your company laptop, our logical systems or physical premises
- Should you have given us written consent to proceed with an employment security screening, as your employer, we need to follow employment due diligence and legal obligations, to comply with specific customers' requirements:
    - Anti-money Laundering Legislation (“AML”).

  - Access to Critical National Infrastructure assets (See https://www.cpni.gov.uk/pre-employment-screening).
  - PCI-DSS Requirement 12.7.
- In addition, If you have asked us to process your request to HR (Careers, Abuse, etc.), we need to process your request, understand your professional experience, capabilities and skills to be discussed internally.
- Note that in particular for applicants, specific data should not be collected about their age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sexual orientation or any other protected characteristic under The Equality Act 2010 (See https://www.eoc.org.uk/).

Contact request administration:

- If you are a potential customer, reseller, partner or any other stakeholder, and you send us a request, we need to process your request before entering into a contract and/or agreement (e.g. provide a quote, you need to contact our different departments - accounting, HR, Marketing, Sales).
- The provision of personal data part of a legitimate interest and possible consequences of failing to provide personal data is our inability to deal with your contact request.

Customer/Suppliers orders, shipping goods or services delivering:

- If you are an existing customer making use of our Network Services, Cloud Services, Communications and Security services), we need to fulfil our contractual obligations to you - your written instructions to provide support for your servers, email and hosting services, backups, security services etc.
- We MAY need to send you emails and communications (e.g. service, technical and other administrative emails, privacy notices updates, messages or phone calls about changes in our services, and important service-related notices, such as security and performance notices. These communications are considered part of the services and you may not opt out of them.
- The provision of personal data is a contractual requirement. Additional processing of personal data is a requirement of our Supplier Data Processing Agreement.
- Possible consequences of failing to provide personal data is our inability to fulfil our contractual obligations to you.

IT infrastructure performance and security incidents handling:

- Note that we may process your personal information as visitor IP address and location for carefully considered and specific performance and security purposes. This enable us to enhance the availability, performance and security of the services we provide but which we believe also benefit our stakeholders (customers, suppliers, employees etc.).
- The provision of personal data is part of a legitimate interest and possible consequences of failing to provide personal data is our inability grant you access to our non-public website pages or systems.
- If you are a user requesting access to our IT infrastructure or physical premises, then as specified in our IT security policies, we need to process your personal data to:

  - Prevent unauthorized access to our physical or information assets.
  - Prevent a data breach.
  - Prevent fraud.
  - Detect intrusion.
  - Prevent malware.
  - Prevent data leak.
  - Prevent a number of specific threats as denial of service attacks.
- Note that If you are an employee from Sensical and your role (e.g. Sensical System Administrator) requires access to information assets located on our servers or our customers' servers, then as your employer, we need to process additional specific personal data (e.g. credentials and location for multi-factor authentication).
- Note that in case of a physical visit to our premises we may also process your name and details of the visit for your safety (e.g. in case of evacuation).

Legitimate B2B marketing communication purpose of processing:

- As part of the Company's legitimate interest B2B communication strategy , we MAY process your personal information, for carefully considered and specific purposes, which are in our interests and enable us to enhance the services we provide, but which we believe also benefit our customers; e.g. to better understand how we are dealing with your information requests, to communicate to you relevant business information about our services.
- The provision of personal data is considered as a legitimate interest and possible consequences of failing to provide personal data is our inability to communicate to you and improve the quality of service we deliver to you.

Consent based B2B marketing communication:

- As part of the Company's consent based B2B communication strategy, we process strictly under your written consent, your personal information for certain business purposes, which include a better understanding how people interact with our websites to enhance our services, to determine the effectiveness of promotional campaigns and advertising, to filter the information we send you according with your interests.
- The provision of personal data part of a legitimate interest and possible consequences of failing to provide personal data is our inability grant you access certain areas to carry out certain tasks above for your benefit.

4. What we do with it

When we act as Data Controller:

When we act as data controller we MAY appoint a data processor and sign a Supplier Data Processing Agreement (“DPA”). This means our appointed data sub-processor cannot do anything with your personal information unless we have instructed them to do it. We only use processors, for the same purpose of processing we have agreed with you and only those processors that provide sufficient guarantees to implement appropriate technical and organisational measures as required by GDPR.

Note that the core activity of Sensical does not consist of processing operations which require regular and systematic monitoring of data subjects on a large scale.

Note that you are not subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning to you or significantly affects you.

Note that it is not part of our processing activities to monitor publicly accessible areas on a large scale, especially when using optic-electronic devices.

Use of Processors and Sub-processors

Sensical has a process in place to inform the data subject of any possible use of processors or sub-processors that have access to your personal data. You can subscribe to receive emails with our privacy policy update as well as our list of approved processors.

Data sharing obligations

Under GDPR there are circumstances where we have a legal obligation to share your data e.g. If you are an employee from Sensical, as your employer we need to process personal data to comply with our legal obligation to disclose employee salary details to HMRC.

Cross-Border Data Transfers

Cross-Border Data Transfers are prohibited, unless certain conditions are met. A Cross-Border Data Transfer MAY be made, on the basis that you have given us explicit consent and we have informed you of the possible risks of such transfer.

However, we MAY use processors that require the transfer of your personal data to a third country outside the European Economic Area (EEA), only when the European Commission has decided that such third country ensures an adequate level of data protection (an "Adequate Jurisdiction")*.

*Note that on July 12, 2016, the European Commission deemed the EU-U.S. Privacy Shield Framework adequate to enable data transfers under EU law (see https://www.privacyshield.gov/Program-Overview and the adequacy determination https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en). The decision by a U.S.-based organization to join the Privacy Shield program (e.g. Microsoft Corporation - Azure cloud services and Office 365) is entirely voluntary. However, once an eligible organization publicly commits to comply with the Privacy Shield Principles through self-certification, that commitment is enforceable under U.S. law by the relevant enforcement authority, either the U.S. Federal Trade Commission (“FTC”) or the U.S. Department of Transportation (“DOT”).

We MAY use the following list of US based processors among the Privacy Shield listed ones (See https://www.privacyshield.gov/list):

Name of Entity	Entity Type/Service Provided	Location	Contact	Privacy Notice
Microsoft Corporation	Cloud Services Office 365	EEA and US	Brendon Lynch Chief Privacy Officer Microsoft Corporation One Microsoft Way Redmond, Washington 98052 brendon.lynch@microsoft.com	https://privacy.microsoft.com/en-gb/privacystatement
Dropbox Inc	Cloud Services Storage	EEA and US	Robin Moore Legal Counsel Dropbox, Inc. Legal Department 333 Brannan Street San Francisco, California 94107 privacy-shield-officer@dropbox.com	https://www.dropbox.com/privacy
Google LLC	Cloud services Storage Consent based Analytics	EEA and US	Keith Enright Director, Privacy Legal Google LLC Google Data Protection Office 1600 Amphitheatre Pkwy Mountain View, California 94043 data-protection-office@google.com	https://policies.google.com/privacy?hl=en&gl=uk

Company Staff administration

Your personal data is processed by Sensical, located in the United Kingdom. Hosting and storage of your data takes place in our Data Centres, which are located in the EEA, predominantly in the United Kingdom.

We MAY use the following list of processors:

Note that if you are an employee from Sensical Services Ltd your personal data included in the payroll data may be processed by 3rd party processors that have access to controller personal data.

Name of Entity	Entity Type/Service Provided	Location	Contact	Privacy Notice
PBA Accountants	Accountants	UK	Rambury House, 18 Charham Lane, Hungerford RG17 0EY	http://www.pbaaccountants.co.uk/terms-and-conditions#privacystatementfull
Dropbox Inc	Cloud Services Storage	EEA and US	Legal Counsel Dropbox, Inc. Legal Department 333 Brannan Street San Francisco, California 94107 privacy-shield-officer@dropbox.com	https://www.dropbox.com/privacy
The Office Group	Office Space	EEA	TOG The Office Group The Office Group The Smiths Building 179 Great Portland Street London	Processor privacy statement can be found at https://www.theofficegroup.co.uk/privacy-policy/

			W1W 5PL dpo@theofficegroup.co.uk	
Microsoft	Office 365 Applications	US and EEA	Microsoft Ireland Operations, Ltd. Attn: Data Protection One Microsoft Place South County Business Park Leopardstown Dublin 18 D18 P521	https://products.office.com/en-gb/business/office-365-trust-center-privacy https://privacy.microsoft.com/en-gb/privacystatement https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located https://www.microsoft.com/en-us/trustcenter/Compliance/EU-Model-Clauses http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=13655
CV Insight	Background screening	EEA	Compliance Team CV Insight Ltd 1 Lea Business Park Lower Luton Road HARPENDEN AL5 5EQ	https://www.cvinsight.co.uk/privacy-policy-data-protection-notice/

Contact request administration

Your personal data is processed by Sensical, located in the United Kingdom. Hosting and storage of your data takes place in our Data Centres, which are located in the EEA, predominantly in the United Kingdom.

Servicedesk - Note that when you call our servicedesk, our telephone equipment usually displays Caller ID ("CLID") information. We use this information to help improve our efficiency and effectiveness dealing with your requests.

We MAY use the following list of processors:

Name of Entity	**Entity Type/Service Provided**	**Location**	**Contact**	**Privacy Notice**
LinkedIn Ireland Unlimited Company	connect with professionals	EU and US	Wilton Place, Dublin 2, Irland	https://www.linkedin.com/legal/privacy-policy
Twitter International Company	News	EU and US	Attn: Privacy Policy Inquiry One Cumberland Place, Fenian Street Dublin 2, D02 AX07 IRELAND	https://twitter.com/en/privacy

Social media - Note that If you are a social media platform user, you are entering into the User Agreement with the social media platform and if you send us a private or direct message via our social media account (e.g. Twitter or LinkedIn), you consent to the collection, use and sharing of your personal data under their privacy policy.

Customer/Suppliers orders, shipping goods or services delivering:

Your personal data is processed by Sensical, located in the United Kingdom. Hosting and storage of your data takes place in our Data Centres, which are located in the EEA, predominantly in the United Kingdom.

We MAY use the following list of processors:

Name of Entity	Entity Type/Service Provided	Location	Contact	Privacy Notice
DHL International (UK) Limited	Goods delivery	EEA and US	Southern Hub Unit 1, Horton Road Colnbrook Berkshire SL3 0BB	https://www.logistics.dhl/gb- en/home/footer/privacy-notice.html
Worldpay (UK) Limited	payment data (e.g. Credit card data) is processed by PCI-Compliant 3rd party Payment processors, through an online merchant account.	EEA and US	The Walbrook Building 25 Walbrook EC4N 8AF London	https://www.worldpay.com/uk/privacy-policy https://www.worldpay.com/uk/worldpay-cookies
Slack	Delivery Team communications	EEA and US	Slack Technologies Limited 4th Floor, One Park Place Hatch Street Upper Dublin 2, Ireland	https://slack.com/privacy-policy https://slack.com/security-practices https://slack.com/privacy-policy-updated#contact
Asana	Project management tool	EEA and US	1550 Bryant Street, Suite 800, San Francisco, CA 94103. terms-questions@asana.com.	https://asana.com/terms#privacy-policy
Microsoft	Office 365 Applications	US and EEA	Microsoft Ireland Operations, Ltd. Attn: Data Protection One Microsoft Place South County Business Park Leopardstown Dublin 18 D18 P521	https://products.office.com/en-gb/business/office-365-trust-center-privacy https://privacy.microsoft.com/en-gb/privacystatement https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located https://www.microsoft.com/en-us/trustcenter/Compliance/EU-Model-Clauses http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=13655

- **Delivering services as Data Processor**

  When under our contract you act as a data controller and we as your appointed data processor, then our mutually signed Supplier Data Processing Agreement ("DPA"), describes any approved sub-processors we MAY use, the purpose of processing you require, the lawful basis you have for that processing, a list of personal data types, a list of sensitive data types, number of records and security controls agreed between both parts depending on the risk level and the service you are using.

Note that no third party sub-processors have access to your data, unless you provide your consent or specifically required by law.

Note that under GDPR, we, the data processor must inform you, the data controller, when data is being moved outside the EEA.

Company IT Systems performance and security events monitoring:

Your personal data is processed by Sensical, located in the United Kingdom. Hosting and storage of your data takes place in our Data Centres, which are located in the EEA, predominantly in the United Kingdom.

We MAY use the following list of processors:

Syslogs are centralized on a server. These can be informational messages, such as user login events, or they can be critical messages, such as a failure in the primary application. These messages play an important part in a network administrator's toolset; they alert the administrator of errors and warnings as they happen, allowing them to respond to problems and fix them. Syslog messages are also provide a method of security auditing.

Name of Entity	Entity Type/Service Provided	Location	Contact	Privacy Notice
Microsoft	Office 365	US and EEA	Microsoft Ireland Operations, Ltd. Attn: Data Protection One Microsoft Place South County Business Park Leopardstown Dublin 18 D18 P521	https://products.office.com/en-gb/business/office-365-trust-center-privacy https://privacy.microsoft.com/en-gb/privacystatement https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located https://www.microsoft.com/en-us/trustcenter/Compliance/EU-Model-Clauses http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=13655

Legitimate B2B marketing communication:

Your personal data is processed by Sensical, located in the United Kingdom. Hosting and storage of your data takes place in our Data Centres, which are located in the EEA, predominantly in the United Kingdom.

Note that your personal data may be processed by means of standard cloud services applications Office 365 provided by 3rd party processors:

Name of Entity	Entity Type/Service Provided	Location	Contact	Privacy Notice
Microsoft	Office 365 (email, word processor services)	EEA and US	Microsoft Ireland Operations, Ltd. Attn: Data Protection One Microsoft Place South County Business Park Leopardstow	https://products.office.com/en-gb/business/office-365-trust-center-privacy https://privacy.microsoft.com/en-gb/privacystatement https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located https://www.microsoft.com/en-us/trustcenter/Compliance/EU-Model-Clauses http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=13655

			n Dublin 18 D18 P521	

Consent based B2B marketing communication:

Your personal data is processed by Sensical, located in the United Kingdom. Hosting and storage of your data takes place in our Data Centres, which are located in the EEA, predominantly in the United Kingdom.

We MAY use the following list of processors:

Name of Entity	Entity Type/Service Provided	Location	Contact	Privacy Notice
Microsoft	Office 365	EEA and US	Microsoft Ireland Operations, Ltd. Attn: Data Protection One Microsoft Place South County Business Park Leopardstown Dublin 18 D18 P521	https://products.office.com/en-gb/business/office-365-trust-center-privacy https://privacy.microsoft.com/en-gb/privacystatement https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located https://www.microsoft.com/en-us/trustcenter/Compliance/EU-Model-Clauses http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=13655
LinkedIn Ireland Unlimited Company	Social Media	EEA and US	Wilton Place, Dublin 2, Irland	https://www.linkedin.com/legal/privacy-policy
Twitter International Company	Social Media	EEA and US	Attn: Privacy Policy Inquiry One Cumberland Place, Fenian Street Dublin 2, D02 AX07 IRELAND	https://twitter.com/en/privacy

Social media - Note that If you are a social media platform user, you are entering into the User Agreement with the social media platform and if you send us a private or direct message via our social media account (e.g. Twitter or LinkedIn), you consent to the collection, use and sharing of your personal data under their privacy policy.

5. How long we keep it

Sensical process personal information only for as long as it is necessary for the fulfilment of the purpose for which the personal information was collected, unless otherwise required or authorised by applicable law.

Our "Data Retention Policy" and "Data Retention Schedule" define how long we keep the information we collect depending on the following processing activities:

Company Staff administration:

For contractual necessity, if you have applied for a job vacancy, we keep applicants personal data for **a maximum 1 year**, according to our Data Retention Policy. After this period, your personal data will be irreversibly destroyed.

On the basis that you have consented the collection of specific data, we keep your data **while you are an employee and as necessary afterwards, on condition that you continue to provide us consent**.

For compliance with legal obligations, we are required to keep staff payroll(3) documents **for 3 years** from the end of tax year they relate to, according to the Data Retention Policy. After this period, your personal data will be irreversibly destroyed.

(3)PAYE and payroll for employers (https://www.gov.uk/paye-for-employers/keeping-records): 3 years from the end of tax year they relate to. HMRC may check the records to make sure the right amount of tax is paid. HMRC Penalties of up to 3,000 GBP apply.

Contact request administration:

Any personal data held by us for contact administration will be kept by us for **a maximum 1 year**, according to our Data Retention Policy or **as long as you provide us consent**.

Note that social media direct messages and non-public communications features of Twitter follow a data retention policy described in https://twitter.com/en/privacy. Take into account that after 30 days from a Twitter account deactivation request, Twitter begins the process of deleting the account, which can take up to a week.

Note that social media you have shared with others via LinkedIn (e.g. through InMail, updates or groups posts) will remain visible after you closed your account or deleted the information from your own profile or mailbox, and LinkedIn does not control data that other Members copied out of our Services.

Customer/Suppliers orders, shipping goods or services delivering:

Personal data types collected in order to enter into or perform a contract with you being the point of contact of your organization (e.g. order / goods shipping or services delivering) will be kept by us for up to **a maximum 7 years**, after terminating the contract, according to our Data Retention Policy.

- **Delivering services as Data Processor**

  When under our contract you act as a data controller and we as your appointed data processor, then our mutually signed Supplier Data Processing Agreement (“DPA”), describes any specific data retention requirements.

Company IT Systems performance and security events monitoring:

Any personal data held by us for system performance and security monitoring will be kept by us for **a maximum of 3 years**, according to our Data Retention Policy. Note that retention policies for On-line Identifiers as cookies or similar technologies, are short periods (measured typically in hours) and are explained in the following sections.

Visitor book logs will be kept **at least 3 months and for a maximum 1 year**, according to our Data Retention Policy.

Legitimate B2B marketing communication:

Any personal data held by us for marketing and service update notifications will be kept by us for **a maximum 1 year**, according to our Data Retention Policy or **as long as you provide us consent**.

Consent based B2B marketing communication:

Any personal data held by us for consent based marketing communications will be kept by us for **a maximum 1 year**, according to our Data Retention Policy or **as long as you provide us consent**.

6. What are your rights?

The GDPR provides the following rights for individuals (see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/). In this section, we provide initial guidance for you in order to identify your rights.

1. The right to be informed (Article 12 GDPR).

2. The right of access (Article 15 GDPR). You shall have the rights to obtain from us confirmation as to whether or not personal data concerning you are being processed and access the personal data.

3. The right of rectification (Article 16 GDPR). You shall have the rights to obtain from us without undue delay the rectification of inaccurate personal data concerning to you.

4. The right to erasure - right to be forgotten (Article 17 GDPR) - (e.g. when the individual withdraws consent). You shall have the right to obtain from us the erasure of personal data concerning to you.

5. The right to restrict processing. (Article 18 GDPR). The data subject shall have the right to obtain from the controller restriction of processing and with the exception of storage, only be processed with the data subject's consent.

6. The right to data portability (Article 20 GDPR). The data subject shall have the right to receive the personal data concerning him or her, in a structured, commonly used and machine readable format and have the right to transmit the data to another controller.

7. The right to object (Article 21 GDPR). You shall have the right to object at any time to processing of personal data concerning you.

8. Rights in relation to automated decision-making and profiling (Article 22 GDPR). The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects him.

9. Right to lodge a complaint with a supervisory authority (Article 77 GDPR). You shall have the right to lodge a complaint with a supervisory authority if you consider that the processing of personal data relating to you infringes GDPR.

Should you believe that any personal data we hold on you is incorrect or incomplete, you have the ability to request to see this information, rectify it or have it deleted. Please contact us using the email address compliance@sensical.net or in writing to our registered office.

In the event that you wish to complain about how we have handled your personal data, please contact the Compliance Team using the email address compliance@sensical.net. Our Compliance Team will then look into your complaint and work with you to resolve the matter.

If you still feel that your personal data has not been handled appropriately, you can contact the Information Commissioner's Office (https://ico.org.uk/) and file a complaint with them.

You can read more about your data protection rights here - https://ico.org.uk/for-the-public/is-my-information-being-handled-correctly/

7. How to manage cookies collected from Sensical.net website visitors

When we provide services, we want to make them easy, useful and reliable. Where services are delivered on the internet, this sometimes involves placing small amounts of information on your device, for example, computer or mobile phone. These include small files known as cookies. In accordance with GDPR, cookies and online identifiers are considered personal data because potentially they may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

These pieces of information are used to improve services for you through, for example:

Enabling a service to recognise your device so you do not have to give the same information several times during one task.

Recognising that you may already have given a username and password so you don’t need to do it for every web page requested measuring how many people are using services, so they can be made easier to use and there’s enough capacity to ensure they are fast.

You can manage these small files yourself and learn more about them through Internet browser cookies - what they are and how to manage them (https://www.gov.uk/help/cookies)

There are two types of cookie you may encounter when using www.sensical.net :

- First party cookies: these are our own cookies, controlled by us and used to provide information about usage of our site.

- Third party cookies: these are cookies found in other companies' internet tools which we are using to enhance our site, for example Facebook or Twitter have their own cookies, which are controlled by them.

First party cookies:

The Sensical.net website (www.sensical.net) uses cookies in several places - we have listed each of them below with more details about why we use them and how long they will last.

Name	Purpose	Typical Content	Expires
JSESSIONID	Allow the Sensical.net website to identify a single user who accesses multiple pages of the Sensical.net website. Allows the user to maintain a shopping cart and remain logged in to the customer control panel.	Unique identification code (does not contain any personal information).	24 hours

Third party cookies:

We use a number of suppliers who may also set cookies on their websites. The control and the dissemination of these cookies is explained by each third-party privacy policy. Please check the third party websites updated information about these 3rd party cookies.

3rd Party Provider	Name	Typical Purpose	Expiration & More info
Google Analytics	utma _utmb _utmc _utmz	These cookies are used to collect information about how visitors use our site. We use the information to compile reports and to help us improve the site. The cookies collect information in an anonymous form, including the number of visitors to the site, where visitors have come to the site from and the pages they visited.	https://www.google.com/intl/en_uk/policies/privacy/ To opt out of being tracked by Google Analytics across all websites visit https://tools.google.com/dlpage/gaoptout

How to control and delete cookies:

If you wish to restrict or block the cookies which are set by our website, or indeed any other website, you can do this through your browser settings. The "Help" function within your browser should tell you how.

Alternatively, you may wish to visit https://www.aboutcookies.org/ which contains comprehensive information on how to do this on a wide variety of browsers. You will also find details on how to delete cookies from your machine as well as more general information about cookies.

Please be aware that restricting cookies will impact on the functionality of our website - you will not be able purchase services or access the customer control panel.

If you wish to view your cookie code, just click on a cookie to open it. You'll see a short string of text and numbers. The numbers are your identification card, which can only be seen by the server that

gave you the cookie. For information on how to do this on the browser of your mobile phone you will need to refer to your handset manual.

To opt-out of third-parties collecting any data regarding your interaction on our website, please refer to their websites for further information (e.g. https://www.google.com/intl/en_uk/policies/privacy/)

Using our products and services without cookies is also possible. In your browser, you can deactivate the saving of cookies, limit them to particular websites, or set the browser to notify you when a cookie is sent. You can also delete cookies from your PC hard drive at any time (file: "cookies"). Please note that in this case you will have to expect a limited page presentation and limited user guidance. Most web browsers allow some control of most cookies through the browser settings.

To find out more about cookies, including how to see what cookies have been set and how to manage and delete them, visit: youronlinechoices.eu

7. Log files

Log files allow us to record visitors' use of the site. The Sensical.net Support Team puts together log file information from all our visitors, which we use for performance and security monitoring (e.g.: make improvements to the layout or security of the site, based on the way that visitors move around it).

8. How we protect your personal information

We implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

We maintain administrative, technical and physical safeguards designed to protect the personal information we collect, against accidental, unlawful or unauthorised destruction, loss, alteration, access, disclosure or use.

- **Delivering services as Data Processor**
    - When under our contract you act as a data controller and we as your appointed data processor, then our mutually signed Supplier Data Processing Agreement (DPA), describes any specific security requirements. Note that the different layers of security to protect Personal data can be taken by the Data Controller and/or by the Data Processor depending on the service e.g. Physical security and Network security can be implemented by the data Processor whereas Application Security can be implemented by the data Controller.
- **As Data Controller**
    - The following section provide a brief overview of what security controls, as a standard baseline, we maintain to protect your data and ensure confidentiality, integrity and availability. However, we cannot provide detail information about our security controls for obvious security reasons. In addition we MAY increase the security controls to mitigate high risks for specific data, since we apply a risk based approach when protecting your data.

1) **Organizational security measures**
   a) **Security Management**
      i) Security policy and procedures. Roles and responsibilities related to the processing of personal data is clearly defined and allocated in accordance with the security policy.
      ii) Compliance: Sensical holds an industry recognised security certification -Cyber Essentials, certificate no: QGCE984 -which is backed by the UK government, The National Cyber Security Centre (NCSC) and the Financial Conduct Authority (FCA) among other entities. See https://www.cyberessentials.ncsc.gov.uk/.
      iii) Sensical holds the Information Commissioner Office (ICO) certificate ZA372483.
   b) **Incident response and business continuity**
      i) Incidents handling / Personal data breaches.
   c) **Human resources**
      i) Confidentiality of personnel.
      ii) Training.
      iii) Background checks: on all employees before having access to systems.
2) **Technical security measures**
      i) Firewalls to ensure that only safe and necessary network services can be accessed from the Internet.
      ii) Secure configuration to reduce the level of inherent vulnerabilities (e.g. Device hardening).
      iii) User access control to provide access to only those applications, computers and networks actually required for the user to perform their role (e.g. Multifactor Authentication).
      iv) Malware protection to restrict execution of known malware and untrusted software, to prevent harmful code from causing damage or accessing sensitive data.
      v) Vulnerability Assessment and Patch management to ensure that devices and software are not vulnerable to known security issues for which fixes are available.
      vi) Encryption of information at rest and in transit to minimize the risk of data loss or data disclosure by unauthorized users.
      vii) Logging and monitoring events and incidents to prevent a data breach as well as to ensure quick response in case of an incident.
      viii) Application lifecycle security to develop applications with security in mind.
      ix) Data deletion/disposal to protect sensitive information.
      x) Physical security to protect people, assets and information.

9. Users under 16

If you are under the age of 16, please make sure that you obtain a parent or guardian's permission before you place your personal information on the website. Users without this consent are not allowed to provide to us their personal data.

Note that we do not seek, nor do we knowingly process, personal information from children under the age of (16). If you think that we have processed personal information of a child under the age of sixteen (16) please contact our compliance team.

10. Linking to another site from the Sensical.net website

Our website contains links to third party sites. Sensical.net is not responsible for the privacy practices within any of these other sites. You should be aware of this when you leave the Sensical.net website and we encourage you to read the privacy statements on other websites you visit.

11. Changes to this privacy notice

We keep our privacy notice under regular review. If this privacy policy changes in any way, we will place an updated version on this page. You can access the latest version of this Personal Data Protection Privacy notice at [https://www.sensical.net/privacy-policy/]. Regularly reviewing this page ensures that you are always aware of what information we collect, how we use it and under what circumstances. This privacy notice was last updated on 25.05.2018.