InkTec Privacy Policy

InkTec recognizes and respects the privacy rights of individuals with regards to their personal data. This Privacy Policy ("Policy") explains what type of personal data we may collect from you and how we use it.

Your privacy is important to us. If you have any questions concerning InkTec's privacy practices or wish to access or correct personal data that InkTec has collected from you, please contact us as described in the "How to Contact Us" section below.

InkTec is a UK based company operating within the UK and Europe. Our parent company is based in South Korea and the address is InkTec Co. Ltd, 98-12, Neungan-ro, Danwon-gu Ansan-City, Gyeonggi-do, 425-839 Korea. InkTec is registered in England as InkTec, Bulford House, Supergas Industrial Estate, Downs Road, Witney, Oxon OX29 0SZ.

Any information you submit to us will only be used by InkTec or subsidiary and will not be passed on to a 3rd Party without your prior consent.

This Privacy Policy applies to InkTec's website, social media pages and online newsletter request form, as well as other customer instigated enquiries. Any person using these communication methods, either manually or via an automated device or program, shall be considered a "User."

All Users are bound to the terms of this Policy. Your use of InkTec's website and online newsletter request form means you consent to the collection and use of your personal data as described in this Policy.

Personal data we collect and use

InkTec collects personal data to operate effectively and provide you with the best experiences from us. You may provide some of this data directly to InkTec through the online newsletter request form, at events or via telephone enquiries. Wherever required or appropriate, InkTec will obtain consent for the processing of your personal data for the purposes outlined in this Policy.

The type of personal data we collect depends on the interactions you have with InkTec. These may include:

- **Name and contact data:** We may collect your name, company name, job title, postal address, email address, telephone number and other similar contact data
- **Demographic data:** We may collect data about you such as your age, gender, country of origin or residence, and preferred language
- **Interests and favourites:** We may collect data about your professional or personal interests and favourites, such as the websites you visit, etc.
- **Financial data:** We may collect data necessary to process payments, such as a bank account or credit card number.
- **Usage data:** We may collect data about how you and your device interact with us, such as time spent on our website, which pages you have visited etc.
- **Relationship and interaction data:** We may collect data about our discussions and meetings, such as when you contact us for information
- **Location data:** We may collect data about your location, which will be imprecise information for example, a location derived from your IP address or data that indicates where you are located with less precision, such as at a city or postcode level.

How we use personal data

InkTec uses the personal data we collect for a number of purposes:

- to communicate with you regarding any requests you have instigated
- to contact you periodically to provide you with marketing and promotional material
- to send administrative information to you, such as any changes to our services
- to personalise your experience when working with InkTec by presenting products tailored to you

- for our business purposes, such as data analysis, audits, developing new products, determining the effectiveness of our promotional campaigns, conducting surveys, and operating and expanding our business activities
- to better understand how our products and services impact you, to track and respond to any queries or concerns
- to offer special events or promotions – these will have their own privacy policies and/or informed consent forms that explain how personal data you provide will be processed in connection with these events or promotions
- as InkTec believes necessary or appropriate:
    A. under applicable law, including laws outside your country of residence
    B. to comply with legal process
    C. to respond to requests from public or government authorities, including authorities outside your country of residence
    D. to enforce our terms and conditions
    E. to protect our operations
    F. to protect our rights, privacy, safety or property, you or others
    G. to allow us to pursue available remedies or limit the damages that we may incur.

Who we share personal data with

We will only share your personal data, with your consent, to complete any transaction or provide any service that you have requested or authorised. We will not sell, distribute or lease your personal information to third parties unless we have your permission, the company merges/reorganises is acquired or are required by law to do so. This may include laws outside your country of residence, to comply with a subpoena, or a legal process.

If you have requested InkTec's newsletter, then the email address you have provided will be forwarded to MailChimp who provide our email marketing services. MailChimp is a third party data processor who has their own privacy policy to which your data will apply too. Please see https://mailchimp.com/legal/privacy/ for MailChimp's privacy policy.

How and where we store your personal data

InkTec uses secure servers using the Secure Sockets Layer (SSL) protocol for data encryption and decryption to protect data from unauthorised interception. Any personal data provided to InkTec is stored here.

Retention Period

InkTec will retain your personal data for the period necessary to fulfil the purposes outlined in this Policy unless a longer retention period is required or permitted by law. You have the right to know and inquire about what personal data we have collected about you. In addition, you have the right to request correction or deletion of such personal data. Please see our Data Protection Policy for more details. Your email address will remain with MailChimp for as long as InkTec use their services for email marketing or you specifically request to be removed from the distribution list. You can do this via the unsubscribe links contained in the newsletters or request removal via communication methods outlined in the 'How to Contact Us' section of this policy. While your email address remains within the MailChimp database, you will receive periodic (approximately 15 times a year) newsletter-style emails from us.

Children

While in some instances we may collect personal data about children this will only be when provided by and consent given by a parent or guardian. Subscribing to InkTec's newsletter is for people over 16 years of age. InkTec does not otherwise knowingly solicit data from, or market to, children. If a parent or guardian becomes aware that his or her child has provided us with personal information, he or she should contact us as described in the "How to Contact Us" section below to enable us to action deletion of such personal data. We will take reasonable steps to delete such information from our database within a reasonable time.

Notification Procedures
In the event your personal data is accessed, lost, or stolen by an unauthorised third party, InkTec will make efforts to notify you to the extent required by law. InkTec will disclose to you the personal data that was accessed/disclosed using the contact information you will have previously provided to us.

Social networks
InkTec is visible on social networking sites and may gain your personal data via your interaction with the InkTec pages. InkTec may follow up any posts on social networking sites and follow the correct procedures regarding obtaining personal data from you if you have not already given it to us. When using social networking sites, please be careful about what personal data you share with others.

External websites
InkTec website includes both internal and external websites. The external website links that InkTec suggests are relevant to the content that they are linking from or are useful for our visitors. InkTec is not responsible for the content on external websites that are linked to from our site. InkTec do not link to external sites in return for cash, services or any other payment in kind – links are selected purely based on the relevance of their content for our audience.

Cookies
Cookies are files sent by web servers to web browsers, and stored by the web browsers. The information is then sent back to the server each time the browser requests a page from the server. This enables a web server to identify and track web browsers. InkTec uses open source analytics software from SAS. This measures the performance of our site and to ensure that it best meets our visitors' needs. Google Analytics are used to compile information about visitors' use of the domain, statistical reports on website activity, and provide other services related to the site and internet use activity. The information is completely anonymous and InkTec cannot track who the user is.

The following cookies are used on our website:

- _utma, _utmb, _utmc and _utmz – used for our Google Analytics. _utmc is a temporary cookies and is deleted once your browser is shut.
- PHPSESSID – a temporary cookie and is deleted once your browser is shut.

The InkTec website uses cookies that do not contain any information that personally identifies you, and does not give InkTec access to your computer or any information about you.

You have a variety of tools to control cookies and similar technologies, including browser controls to block and delete cookies:

In Internet Explorer, you can refuse all cookies by clicking "Tools", "Internet Options", "Privacy", and selecting "Block all cookies" using the sliding selector.

In Firefox, you can adjust your cookies settings by clicking "Tools", "Options" and "Privacy". Blocking cookies will have a negative impact upon the usability of some websites.

Your browser settings may impact your experience on the InkTec website.

InkTec's cookies provide services and help collect data. This data allows InkTec to, among other things, identify your IP address, browser type, domain name, referring URL's, store your preferences and settings and in future, if a secure log in areas developed on our website, enable you to sign-in easier, allow us to recognise you when you return to our site and provide you with a more customised experience.

How to Contact Us
InkTec is happy to answer any questions or comments you may have regarding this Policy or its implementation. Please use the contact details below. We will use reasonable efforts to resolve or address

your concern. Please note that email communications are not always secure, so please do not include sensitive information in your emails to us.

InkTec
Bulford House
Supergas Industrial Estate
Downs Road
Witney
Oxon OX29 0SZ

Tel: 01993 862 770
info@inkteceu.com

Updates to our Privacy Policy

InkTec may update this Policy from time to time. Please check this Policy periodically for changes. If we make any changes, the updated Policy will be posted with a revised effective date. We encourage you to periodically review this page for the latest information on our privacy practices.

Your continued use of our Services following the posting of changes to the Policy will mean you accept those changes.

InkTec Data Protection Policy

InkTec needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards and ensure it is GDPR compliant.

This data protection policy ensures InkTec:

- complies with data protection law and follow good practice
- protects the rights of staff, customers and partners
- is open about how it stores and processes individuals' data
- protects itself from the risks of a data breach

Data Protection law
The Data Protection Act 1998 describes how InkTec must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. The Data Protection Act is underpinned by eight important principles. These say that personal data must be:

- processed fairly and lawfully
- obtained only for specific, lawful purposes
- adequate, relevant and not excessive
- accurate and kept up to date
- not be held for any longer than necessary
- processed in accordance with the rights of data subjects
- protected in appropriate ways
- not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

GDPR enhancements to the Data Protection Law
GDPR is Europe's new framework for data protection laws. Each member state in the EU operates under the current 1995 data protection regulation and has its own national laws. In the UK, the current Data Protection Act 1998 sets out how your personal information can be used by companies, government and other organisations.

GDPR changes how personal data can be used. Its provisions in the UK will be covered by a new Data Protection Bill, however these include everything in the GDPR. The main enhancements are:

- companies will be more accountable for handling of personal data
- if someone wishes to access their personal data, this can be provided free of charge (previously £10) and it must be provided within one month
- everyone will have the right to get confirmation that an organisation has information about them, access to this information and any other supplementary information, amend/delete/object to certain data uses, of their personal data
- the right of portability (individuals requesting their personal data being held by one company be transported to another)
- consent will need to be obtained from individuals for every usage of their personal data
- stricter processing requirements of which individuals can receive information on this processing of their personal data
- GDPR applies to all organizations established in the EU or processing data of EU citizens, which broads the scope of EU data protection law well beyond the borders of just the EU

International
InkTec Europe's parent company is based in South Korea. All data for InkTec Europe is processed in the UK and is the lead data protection supervisory authority for data provided in the UK. There is no cross border processing of data.

Policy Scope
This policy applies to InkTec including all staff, contractors and suppliers working on behalf of InkTec. It applies to all data that we hold relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998 (and the new Data Protection Bill 2018). This includes all personal data including:

- names
- postal addresses
- email addresses
- telephone numbers
- plus any other identifiable information

Data Protection Risks
This policy helps to protect InkTec from very real data security risks including:

- Breach of confidentiality: such as information being given out inappropriately
- Failing to offer choice: such as all individuals should be free to choose how InkTec uses data relating to them
- Reputational damage: for instance, InkTec could suffer if hackers successfully gained access to sensitive data

If a data breach occurs, and the breach is likely to result in the risk to the rights and freedom of individuals, then InkTec has the duty to report it to the Information Commissioners Office (ICO).The individuals whose data has been breached will also be notified and appropriate steps taken to fix the issue in a timely manner. However, the procedures InkTec's has put in place should effectively detect, report and investigate personal data breaches before they occur.

How we protect your personal data
Everyone who works for, or with, InkTec has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and its data protection principles.

Personnel with key areas of responsibility:

- Board of Directors: to ensure InkTec meets it legal obligations

- Data Protection Officer:
    - responsible for data protection compliance
    - reviewing the data protection policy
    - manage data protection training
    - handle questions from staff
    - keeping the board updated about data protection responsibilities, risks and issues
    - reviewing all data protection procedures and related policies, in line with an agreed schedule
    - arranging data protection training and advice for the people covered by this policy
    - handling data protection questions from staff and anyone else covered by this policy
    - dealing with requests from individuals to see the data InkTec holds about them (subject access requests)
    - checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The IT Manager:

- ensuring all systems, services and equipment used for storing data meet acceptable security standards
- performing regular checks and scans to ensure security hardware and software is functioning properly
- evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

- The Marketing Manager:
  - approving any data protection statements attached to communications such as emails and letters
  - addressing any data protection queries from journalists or media outlets
  - where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

InkTec has implemented a variety of security technologies and organisational procedures to protect your personal data from unauthorised access, use and disclosure.

Staff Guidelines

- The only employees able to access data covered by this policy are those who need it for work
- Data is not shared informally. When access to confidential information is required, employees can request it from their line managers
- InkTec will provide training to all employees to help them understand their responsibilities when handling data
- Employees will keep all data secure, by taking sensible precautions and following the guidelines below
- In particular, strong passwords are used and never be shared
- Personal data will not be disclosed to unauthorised people, either within the company or externally
- Data is regularly reviewed and updated if it is found to be out of date. If no longer required, it is deleted and disposed of
- Employees will request help from their line manager or the Data Protection Officer if they are unsure about any aspect of data protection.

Once this data protection policy has been read and training received, all staff members will sign a data protection policy training form to show they are compliant, which will then be stored on their own HR file. Any training given due to updates to the data protection policy will also be recorded on this form.

Where we store and process personal data
InkTec Europe is a UK based company so your personal data is stored and processed in the UK on servers based in the UK. InkTec takes steps to process personal data according to the provisions of this Policy and the requirements of applicable law.

InkTec stores your data safely. When data is stored on paper, it is kept in a secure place where unauthorised people cannot see it. This applies to data that is usually stored electronically but has been printed out for some reason:

- when not required, the paper or files will be kept in a locked drawer or filing cabinet
- employees will make sure paper and printouts are not left where unauthorised people could see them, like on a printer
- data printouts will be shredded and disposed of securely when no longer required
- when data is stored electronically, it will be protected from unauthorised access, accidental deletion and malicious hacking attempts
- data will be protected by strong passwords that are changed regularly and never shared between employees
- if data is stored on removable media (like a CD or DVD), these will be kept locked away securely when not being used

- data will only be stored on designated drives and servers, and will only be uploaded to an approved cloud computing services
- servers containing personal data are sited in a secure location, away from general office space
- data is backed up frequently. Those backups are tested regularly, in line with the company's standard backup procedures
- data will never be saved directly to laptops or other mobile devices like tablets or smart phones
- all servers and computers containing data are protected by security software and a firewall

Data Use
Personal data is of no value to InkTec unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- when working with personal data, InkTec employees will ensure the screens of their computers are always locked when left unattended
- personal data is not shared informally. In particular, it is never sent by email, as this form of communication is not secure
- data is encrypted before being transferred electronically. InkTec's IT Manager ensures that all InkTec staff know how to send data to authorised external contacts
- personal data is never transferred outside of the European Economic Area
- employees will not save copies of personal data to their own computers. Staff will always access and update the central copy of any data.

Data Accuracy
InkTec takes take reasonable steps to ensure data is kept accurate and up to date in accordance with the law.

The more important it is that the personal data is accurate, the greater the effort InkTec will put into ensuring its accuracy. It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff will not create any unnecessary additional data sets
- Staff will take every opportunity to ensure data is updated, such as confirming a customer's details when they call
- InkTec will make it easy for data subjects to update the information InkTec holds about them
- Data is updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the Marketing Manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

Subject Access Requests (How you can access and control your personal data)
You have choices about the data InkTec collects. When you are asked to share your personal data with InkTec, you may decline; however, your choice not to share your personal data with InkTec may mean you will not be able to use or (fully) benefit from our services or offerings.

InkTec respects your right to know and inquire about what personal data you have provided to us. In addition, you have the right to request correction or deletion of such personal data, as well as to request removal of your personal data and to be kept informed how the InkTec is meeting its data protection obligations. This is a Subject Access Request.

If you would like to make a request for InkTec to correct or delete personal data that you have provided to us, please contact us as described in the "How to Contact Us" section below and we will respond in a reasonable time. We will make a good faith effort to provide you with access to your personal data and to correct any inaccuracies or delete such information at your request, if it is not otherwise required to be retained by law.

InkTec may decline to process requests that are unreasonably repetitive or systematic, require disproportionate technical effort or jeopardise the privacy of others. Before fulfilling your requests, InkTec may need to verify your identity.

Data Protection Impact Assessments
InkTec will conduct a Data Protection Impact Assessment to adhere with the law when relevant. This maybe if new technology is deployed or where a profiling operation is likely to significantly affect individuals. If InkTec feel they are unable to address high risks, then they will consult with the ICO to ensure that their processing complies with the law.

InkTec does not hold and therefore does not process special categories of personal data.

Disclosing data
In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, InkTec will disclose requested data. However, the Data Protection Officer will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

How to Contact Us
InkTec is happy to answer any questions or comments you may have regarding this Policy or its implementation. Please use the contact details below. We will use reasonable efforts to resolve or address your concern. Please note that email communications are not always secure, so please do not include sensitive information in your emails to us.

InkTec
Bulford House
Supergas Industrial Estate
Downs Road
Witney
Oxon OX29 0SZ

Tel: 01993 862 770
info@inkteceu.com

Updates to our Data Protection Policy
InkTec may update this Policy from time to time. Please check this Policy periodically for changes. If we make any changes, the updated Policy will be posted with a revised effective date. We encourage you to periodically review this page for the latest information on our data protection practices.