Rayners Data Protection Policy

Rayners 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 Rayners:

- 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 Rayners 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

Policy Scope

This policy applies to Rayners including all staff, contractors and suppliers working on behalf of Rayners. 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 Rayners 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 Rayners uses data relating to them
- Reputational damage: for instance, Rayners 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 Rayners 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 Rayners'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, Rayners 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 Rayners 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 Rayners 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 Sales Marketing & Admin support
    - 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.

Rayners 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
- Rayners 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.

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

Rayners 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 Rayners 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, Rayners 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. Rayners's IT Manager ensures that all Rayners 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
Rayners 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 Rayners 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
- Rayners will make it easy for data subjects to update the information Rayners 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 Director'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 Rayners collects. When you are asked to share your personal data with Rayners, you may decline; however, your choice not to share your personal data with Rayners may mean you will not be able to use or (fully) benefit from our services or offerings.

Rayners 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 Rayners is meeting its data protection obligations. This is a Subject Access Request.

If you would like to make a request for Rayners 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.

Rayners 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, Rayners may need to verify your identity.

Data Protection Impact Assessments
Rayners 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 Rayners feel they are unable to address high risks, then they will consult with the ICO to ensure that their processing complies with the law.

Rayners 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, Rayners 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

Rayners 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.

KP Rayners Ltd
Unit 5b
Wedgwood Road
Bicester
Oxfordshire
OX26 4UL

Please use the Contact Us Form should you have any queries.

Updates to our Data Protection Policy
Rayners 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.