Data Protection Policy (GDPR Compliant)

30.1. This Data Protection Policy sets out how CRATUS LIMITED handle the personal data of our customers, suppliers, employees, workers and other third parties regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other data subject.

30.2. This Data Protection Policy applies to all Company personnel and sets out what we expect from you in order for the Company to comply with applicable law. Your compliance with this Data Protection Policy is mandatory. Any breach of this Data Protection Policy may result in disciplinary action.

30.3. Personal Data Protection Principles

30.4. We adhere to the principles relating to processing of personal data set out in the GDPR which require personal data to be:

a. Processed lawfully, fairly and in a transparent manner
b. Collected only for specified, explicit and legitimate purposes
c. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
d. Accurate and where necessary kept up to date
e. Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed
f. Processed in a manner that ensures its security using appropriate technical and organisational measures
g. Not transferred to another country without appropriate safeguards being in place
h. Made available to data subjects who are allowed to exercise certain rights in relation to their personal data

30.5. We are responsible for and must be able to demonstrate compliance with the data protection principles listed above.

30.6. Lawfulness, Fairness, Transparency

a. Lawfulness and fairness

i. Personal data must be processed fairly and in a transparent manner in relation to the data subject.

i. You may only collect, process and share personal data fairly and lawfully and for specified purposes, some of which are set out below:

A. the data subject has given his or her consent;
B. the processing is necessary for the performance of a contract with the data subject;
C. to meet our legal compliance obligations.

© Copyright The Advocacy Group Limited 2019

D. to protect the data subject's vital interests;

E. to pursue our legitimate interests.

b. Consent

i. A data controller must only process personal data on the basis of one or more of the lawful bases set out in the GDPR, which include consent.

i. A data subject consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing.

i. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

i. Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

i. Consent may need to be refreshed if you intend to process personal data for a different and incompatible purpose which was not disclosed when the data subject first consented.

i. Unless we can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data, for automated decision-making and for cross border data transfers. Usually we will be relying on another legal basis (and not require explicit consent) to process most types of sensitive data. Where explicit consent is required, you must issue a fair processing notice to the data subject to capture explicit consent.

i. You will need to evidence consent captured and keep records of all consents so that the Company can demonstrate compliance with consent requirements.

c. Transparency

i. The GDPR requires data controllers to provide detailed, specific information to data subjects depending on whether the information was collected directly from data subjects or from elsewhere. Such information must be provided through appropriate privacy notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand them.

30.7. Purpose Limitation

30.8. Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

30.9. You cannot use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the data subject of the new purposes and they have consented where necessary.

30.10. Data Minimisation

30.11. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

30.12. You must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

30.13. Accuracy

30.14. Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

30.15. You must check the accuracy of any personal data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

30.16. Storage Limitation

30.17. Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

30.18. You must not keep personal data in a form which permits the identification of the data subject for longer than needed for the legitimate business purpose for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

30.19. You will take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with all the Company's applicable records retention policies. This includes requiring third parties to delete such data where applicable.

30.20. You will ensure data subjects are informed of the period for which data is stored and how that period is determined in any applicable privacy notice.

30.21. Security Integrity And Confidentiality

30.22. Protecting Personal Data

30.23. Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

30.24. You must follow all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction. You may only transfer personal data to thirdparty service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

30.25. You must maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

30.26. Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

30.27. Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

30.28. Availability means that authorised users are able to access the personal data when they need it for authorised purposes.

30.29. Reporting A Personal Data Breach

30.30. The GDPR requires data controllers to notify any personal data breach to the applicable regulator and, in certain instances, the data subject.

30.31. Transfer Limitation

30.32. The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You may only transfer Personal Data outside the EEA if one of the following conditions applies:

a. the country to which we transfer the personal data ensures an adequate level of protection for the data subjects' rights and freedoms;
b. the data subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or
c. the transfer is necessary for one of the other reasons set out in the GDPR

30.33. Data Subject's Rights And Requests

30.34. Data subjects have rights when it comes to how we handle their personal data. These include rights to:

a. withdraw consent to processing at any time;
b. receive certain information about the data controller's processing activities;
c. request access to their personal data that we hold;
d. prevent our use of their personal data for direct marketing purposes;
e. ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
f. restrict processing in specific circumstances;
g. challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
h. request a copy of an agreement under which personal data is transferred outside of the EEA;
i. object to decisions based solely on automated processing, including profiling;
j. prevent processing that is likely to cause damage or distress to the data subject or anyone else;
k. be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
l. make a complaint to the supervisory authority; and
m. in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

30.35. Accountability

30.36. The Data controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The data controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

30.37. Record Keeping

30.38. The GDPR requires us to keep full and accurate records of all our data processing activities.

30.39. Training And Audit

30.40. We are required to ensure all company personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

30.41. Direct Marketing

30.42. We are subject to certain rules and privacy laws when marketing to our customers.

30.43. For example, a data subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). the limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

30.44. The right to object to direct marketing must be explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information.

30.45. A data subject's objection to direct marketing must be promptly honoured. if a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

30.46. Sharing Personal Data

30.47. Generally we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

30.48. We may only share the personal data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

31.Electronic Information and Communications Systems Policy

31.1. Our electronic communications systems and equipment are intended to promote effective communication and working practices within our organisation, and are critical to the success of our business. This policy deals mainly with the use (and misuse) of computer equipment, e-mail, the internet, telephones, smart phones, Blackberries, and voicemail, but it applies equally to the use of fax machines, copiers, scanners, CCTV, and electronic key fobs and cards. It outlines the standards we require users of these systems to observe, the circumstances in which we will monitor use of these systems and the action we will take in respect of breaches of these standards.

31.2. All staff are expected to protect our electronic communications systems and equipment from unauthorised access and harm at all times. Failure to do so may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

31.3. Staff are responsible for the security of the equipment allocated to or used by them, and must not allow it to be used by anyone other than as permitted by this handbook.

31.4. Passwords are unique to each user and must be changed regularly to ensure confidentiality. Passwords must be kept confidential and must not be made available to anyone else unless authorised by the Office Administrator. For the avoidance of doubt, on the termination of employment (for any reason) staff must provide details of their passwords to the Office Administrator and return any equipment, key fobs or cards.

31.5. Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Staff should assume that e-mail messages may be read by others and not include anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain.

31.6. Staff should not access any web page or any files (whether documents, images or other) downloaded from the internet which could, in any way, be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK, it may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of our Electronic Information and Communications Systems Policy.

31.7. Staff should not under any circumstances use our systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information on a blog or wiki, even in their own time.

31.8. We permit the incidental and reasonable use of internet, e-mail and telephone systems to send personal e-mail, browse the internet and make personal telephone calls. Personal use is a privilege and not a right. It must be neither abused nor overused and we reserve the right to withdraw our permission at any time.

31.9. Misuse or excessive use or abuse of our telephone or e-mail system, or inappropriate use of the internet in breach of this policy will be dealt with under our Disciplinary Procedure. Misuse of the internet can, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by participating in online gambling or chain letters or by creating, viewing, accessing, transmitting or downloading any of the following material will amount to gross misconduct (this list is not exhaustive):

a. pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);
b. offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients;
c. a false and defamatory statement about any person or organisation;
d. material which is discriminatory, offensive, derogatory or may cause embarrassment to others;
e. confidential information about us or any of our staff or clients (which you do not have authority to access);
f. any other statement which is likely to create any liability (whether criminal or civil, and whether for you or us); or
g. material in breach of copyright.

31.10. Any such action will be treated very seriously and is likely to result in summary dismissal.