Privacy statement

D8A is committed to protecting your privacy. This privacy Statement explains what information we collect about users of our services and describes how we will use it.

What information do we collect?

D8A collects the following:

Details generated upon initial contact

We collect your personal details during preliminary contact in order to fulfil your initial enquiry, such as performing an audit or providing a quotation.

During our initial audit we are preparing to support your organisation and your users and to such end we obtain information of each of the adult users for automatic entry in our helpdesk system. This will be your full name and email address and this will be used to log cases relating to you as a computer user and to provide you with automatic and manual notifications about the status of open and closed cases.

Upon signing a contract with D8A we require that you nominate one person to be the Company Supervisor and it will be required that this user allow us to store their email address and phone number and use it in order to make contact regarding the IT infrastructure of the contracted company. This user may request that we remove their data from our systems, but this must be immediately replaced by another user.

We also require an accounts contact to be nominated and their data will be used to liaise regarding accounting queries such as sending invoices and statements.

We require that all Company Supervisors have a Dashlane account for us to share the login details of the admin account with which the third-party service can be managed.

It is important that customers carefully consider our advice as often it can only be effective if taken as a whole.

Automated Data Collection

During the use of services provided by D8A, personal Data may be automatically collected. This could be via LDAP integration, Service Requests by email, guest portal and via the D8A website. All methods will create a SysAid account for use in monitoring and processing requests.

We disable user data in our system when users are removed from your system. Data is not permanently removed as you and us have a legitimate interest in keeping records of communications and notes relating to past support cases.

Marketing

We only use your personal information for direct marketing purposes if we can do this by law. We may use your information to notify you about changes to the functionality of services. Company Supervisors are sent mandatory notifications, such as service status messages and planned maintenance.

We may send you offers or information in which we think you may be interested. We may contact you by post or email. Company Supervisors are also initially set up to receive our newsletter and marketing emails which we believe to be relevant information for the user in the role of Company Supervisor. The newsletter and marketing emails can be unsubscribed, whereas the mandatory notifications cannot.

If at any time you decide you no longer want to be contacted by us or to receive offers and information from D8A you can click the unsubscribe link in the communication.

We also purchase data from a third party, Selectabase. They state the following: "Selectabase only provides data that can be processed for direct marketing purposes using legitimate interests as the legal basis. Business to business data for sole traders and true partnerships includes postal and telephone data, and B2B data for corporate entities includes email postal, and telephone data, screened against the Telephone Preference Service (TPS) and Corporate Telephone Preference Service (CTPS)."

You can read more from Selectabase here.

Marketing is a significant and important economic activity. D8A have a legitimate interest in seeking to address marketing to the most relevant audiences.

In all communications we ensure the that unsubscribe options are on all communications and we ensure proper segmentation when delivering communications (e.g. to ensure the data subject would have a legitimate interest in the topic or content of any communication received).

Legal basis for Processing

The legal basis we use to process your personal data may differ for each processing activity.

The personal information that we collect is so that we can provide you with our Support services and products and is processed with your explicit consent.

If we need to contact other agencies in order to provide you with services or products, we shall always gain your consent before sharing your personal data with this third-party.

We have a Legitimate Interest to automatically collect and process data for the purpose of processing support requests and the monitoring of network systems.

The personal information that we collect to fulfil individual employment contracts with our employees is processed under Legitimate Interest.

Our Commitment to Data Security

To prevent unauthorised access, maintain data accuracy, and ensure the correct use of information, we have put in place appropriate physical, electronic, organisational and managerial procedures to safeguard and secure the information we collect.

For more information on our internal procedures please read the following:

Data Protection and Privacy Policy

Data Breach and Information Security Incident Policy and Procedure

All data that we hold is held in a secure environment.

Control of information

All individuals who are the subject of personal data held by D8A are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.
- Know how to request its removal.
- Ask for data not to be used.

If an individual, contacts the company requesting this information, this is called a Subject Access Request.

Subject access requests from individuals should be made by email, addressed to the data controller helpdesk@businessnetworks.co.uk.

Individuals will be charged £10 per subject access request. The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Removal

Individuals have the right to request that we remove the data that we hold for them, only if they are not specified as the Company Supervisor of an organisation that we work with. Please send an email from your own business email address to helpdesk@businessnetworks.co.ukto request that we remove the personal data that we hold for you. If you are a Company supervisor then please provide us with the details of a suitable replacement for the role of Company Supervisor.

Note: We will contact that user to ensure that they consent to taking up the role and us holding their personal information for this purpose.

Correction

Individuals have the right to request that we correct the information that we hold on them. Please send an email from your own business email address to helpdesk@businessnetworks.co.ukto request that we correct that personal data that we hold for you.

User Data Requests

Organisations may also make requests for information held on or stored by their employees, contractors and suppliers. This may include assisting with the retrieval of data held on systems administered by D8A on their behalf.

These requests must be made in adherence to any internal Policies and via Board or Governing body approval. Under no circumstances will such a request be accepted from an individual and independent verification will be sought from the appropriate body.

Disclosing data for other reasons

We may share personal information, as necessary, with our service providers, agents or other relevant third parties so that we can provide the services you have asked for, or to carry out any other obligations arising from any contract or agreement entered into between you and D8A.

When we make a recommendation to use a specific service, such as Office 365, it is important that you understand how your data is held by the third-party organisations and that you liaise with them directly if you have any concerns about how they store and use your data.

Acronis GDPR resource (Backup Services)

Proofpoint GDPR resource (Email Archiving)

Microsoft GDPR resource (Cloud Services and Software vendor)

Cloud2Me (Cloud Services and email hosting)

We do not permit these parties to use such information for any other purpose than to perform the services they have been instructed to provide by us.

We may also need to disclose your information if required to do so by law.

Changes to this privacy notice

We keep our privacy statement under regular review. This privacy statement was last updated on 07/05/2020.