Storganise Ltd - GDPR Policy

Storganise create custom applications for businesses and individuals as a framework for the storage and manipulation of data.

Client (External) Data

In the course of our business, it is sometimes necessary to work with clients' data. In these instances we have a strict set of guidelines to be adhered to.

Clients' data is only to be kept if there is a need for that data to assist with the work in hand.

All external data is kept in a "TDD" or "Temporary Data Drive" - this is a password-protected location that is not backed up. All external data is deleted as soon as it is no longer pertinent to the task.

A calendar entry is set to remind all users to check the TDD monthly (on 10th of the month) to delete any data that is not currently in use.

Marketing and cookies

Our website does not collect data, and does not use cookies as a remarketing tool.

There are three WordPress cookies on the site:

Wordpress_clef_session which improves the website's useability; wp_settings-4 and wp_settings-time-4 which are both performance cookies.

We have two Google Analytics cookies:

_ga which calculates the number of unique users to a website and allocates them a number without identifying them

_gid a 24 hour browsing cooking enabling you to return quickly to the site within a 24 hour period. This cookie expires after 24 hours.

We do not use our previous clients' details for marketing.

For future marketing strategies, we will obtain permission from previous and current clients before sending any marketing materials.

Data Protection Officer

Being a Micro-Organisation, we have not appointed a DPO. Should the company expand, this policy will be changed.

Data Transfer Policy

When data is to be transferred from us to our clients, it will be in any of the following formats…

1 - Password protected and security enabled Filemaker Pro database
2 - Password protected Excel Spreadsheet
3 - Password protected Word Document
4 - Any other password protected document

Password Transfer

Passwords to unlock protected documents must not be communicated via email, or through the same medium as the protected document.

Acceptable methods of Password transfer are…

1 - Face to face with the recipient
2 - Verbally over the phone
3 - Text message if the texts are not intercepted by an email programme (Kapow or Twilio for example)

Client Password Policy

When setting passwords for client access to Applications the “Enforce User to change Password on first login” must be checked.

Company Password Policy

Passwords are never to be written down.
Aide-memoirs can be utilised to remember passwords, and written down in code, as long as they do not reference the Username alongside them.

Subject Access Request

Client data is held in three different areas, which will be provided on request…

1 - Client folder - This is held in the Shared “Storganise” folder, and will be the name of the Client.
2 - TDD Folder - If we have data still current that we are using for the client it will be in a folder in the TDD Folder, in the name of the Client.
3 - Email trail - All mails from the client will be in the Email folder in the name of the client. Sent mails can be provided utilising a search for the Client name, and the names of the client contact(s)