

GDPR Data Audit 1

IR's role as Data Processors in carrying out reception services for Natural Touch Clinic

Date 17th May 2018

Introduction

At IdealReceptionist we are proud of our reputation for providing a highly personalised and professional telephone reception service for our clients in the healthcare professions. We are dedicated to improving our service and maintaining our place at the top of the market in terms of quality and customer care and for this reason we take the impending GDPR legislation very seriously.

On 24th May 2018 the new European wide General Data Protection Legislation comes into force. Under the act, as Data Processors for our clients' it is our duty to compile the following Data Audit which outlines the type of work we carry out and data we handle for our you in **our role managing your diaries and handling your patients' calls** and the processes and security measures we have in place to ensure it is GDPR compliant. The work we carry out and data we handle to provide our service to you as clients is set out in a separate audit; *"GDPR Data Audit 2"*

Should you have any queries about the information provided in this audit or require any additional information, please feel free to contact Tracy Evans at any time.

Natural Touch Clinic

Data Controller

Our Role

Data Processor

Appointed Overseer

Tracy Evans, Operations Manager - Ideal Receptionist is below the required size for a DPO

Data Audit Form	
Type of Data	Patient name, contact number, sometimes date of birth, address, email address, insurance details where applicable. We are able to take patient credit card details if you use a practice management software that has a credit card storing function to store these securely.
Description of data	Basic personal data in order for the practitioner to know who they are treating and how they can contact them.
Employee responsible	All our team members are responsible for recording this data.
Date of consent to hold data	Date of signing up for our services.
Where the data is stored	Data storage is primarily done on Practicepal any other information we handle for your company is sent to you by email through a secure server which is ISO 27001 and cyber essentials protected.
Source of the data	For new patients, their telephone calls to us, for repeat customers, their details on Practicepal practice management system.
Purpose of the data	To enable the practitioner or their clinic to contact the patient and provide treatments.
How the data is protected in its storage	All patient information is stored on the Practicepal diary. all emails are stored on a secure server which is ISO 27001 and cyber essentials protected.
Usage restrictions	All team members have password logins and are signatories to confidentiality agreements with regards to any work carried out for our company and its clients.
Data Subject Requests	Any Data Subject requests should be addressed to Tracy Evans, our Data Protection overseer.
Usage frequency	We access your diary only when carrying out work commissioned for your practice.
Retention period	All emails are deleted after 12 months. Retention of diary information is under the control of the client.

Backup and Disaster Recovery	All our data is stored on cloud by GDPR compliant providers.
Comments	

GDPR Data Audit 2

Handling Client Accounts

Date 17 May 2018

Introduction

As stated in the introduction of “*GDPR Data Audit 1*” we are dedicated to improving our service and we take the impending GDPR legislation very seriously.

Although companies are not outlined as eligible for protection under the act, any information that could identify specific people within those companies is, thus, under the act it is our duty to compile the following Data Audit.

This audit covers the Data Controlling and Processing IdealReceptionist carries out in **our work as service providers for our clients** and the processes and security measures we have in place to ensure we are GDPR compliant. The work we carry out as Data Processors, managing our clients’ diaries and handling their patents calls is set out in a separate audit specifically analysing that task entitled “*GDPR Data Audit 1*”

Should you have any queries about the information provided in this audit or require any additional information, please feel free to contact Tracy Evans at any time.

Ideal Receptionist Data Controller and Processor

Appointed Overseer Tracy Evans, Operations Manager - Ideal Receptionist is below the required size for a DPO

Data Audit Form	
Type of Data	Basic personal (contact names and roles) and practice data
Description of data	Basic personal data in order for us to know who our client is and practice data in order for us to carry out our role efficiently.
Employee responsible	All team members.
Date of consent to hold data	Date of contact with the company
Where the data is stored	FreeAgent, Igloo, Dropbox, Payment solutions, MyOffice.net and practice management software.
Source of the data	Client
Purpose of the data	In order for IR to know who their client is and to carry out the role as though they are working in the practice.
How the data is protected in its storage	MyOffice.Net diaries and all practice management software and igloo we used is secure and password protected. Freeagent, Dropbox and banking all secure with restricted access and password protected. (See appendix for details)
Usage restrictions	All team members have password logins
Data Subject Requests	To be addressed to Tracy Evans, Operations Manager
Usage frequency	Daily use of all systems
Retention period	We hold data for 12 months after a client has left us when there is a potential that they may return.
Backup and Disaster Recovery	Provided by the individual storage and software services.
Comments	The GDPR regulations only concern data that would enable the identification of persons, for example, personal contacts and personal email addresses.

Appendix

Data Protection Security of our storage intranet email and software providers:

IGLOO

“Your data is safe with us.

Igloo works inside and outside your firewall, so whether you’re using Igloo exclusively as an intranet, or you’ve extended permissions to clients and partners outside your company, your data remains secure. It’s hosted in a private cloud and content is delivered securely via the web browser.

Igloo’s enterprise-class security features are constantly monitored and tested. Our platform, processes, and networks regularly undergo independent security audits to ensure our high standards for security are met – and exceeded.

EU GDPR

The General Data Protection Regulation (GDPR) is a new law that will provide greater data protection for individuals in the European Union (EU). If you’re thinking ahead to the EU GDPR, we are too. Igloo is committed to helping our customers comply with the upcoming legislature through our strong foundation of data governance and championing of privacy. Igloo is actively working to be fully compliant with the EU GDPR by the May 25, 2018 enforcement date.

Check back often for more updates.”

DROP BOX

“Welcome to Dropbox's GDPR guidance center

This guidance center hopes to offer some helpful insight and practical steps for organizations as they prepare for compliance with the General Data Protection Regulation, otherwise known as the GDPR, by May 25, 2018.

Of course, every organization’s journey to GDPR compliance is different. It depends on, among other factors, company size, the types and amount of data it processes, and its current security and privacy measures.”

.”

Smart Debit

“At SmartDebit, we are keeping up-to-date with the ICO to be fully prepared for GDPR when it is implemented on 25 May 2018.”

Nasstar

Certified

ISO 27001 and Cyber Essentials protects the integrity of your business information and data.

Also found this article by Nasstar <http://blog.nasstar.com/general-data-protection-regulation-guide/>