GDPR Policy

The Information Commissioner's Office (ICO), tell us that General Data Protection Regulation (GDPR) policies must be written in plain and simple language without any jargon or 'legal speak'.

Aim

The aim of this policy is to ensure we at Forensic Defence, comply with the General Data Protection Regulations (GDPRs) which apply to everyone who holds personal data, from 25th May 2018.

Overview

General Data Protection Regulations (GDPRs) have been made to give individuals more control about what happens to the personal data they provide to our organisations. From 25th May 2018 onwards, your personal data cannot be gathered, stored or processed unless one of the six legal bases apply. Also, it must be destroyed if its purpose has ended. If you request details of any personal data held about you, the company must send it to you without charging you a fee or any other cost. This way, you should know that we have your personal data because you have allowed us to have it, or that we are storing and processing it because of one of the six legal bases.

However, personal data that we have in our records from before the 25th May 2018, will still be valid, but will now become subject to our storage, processing and destruction policy. All non-relevant data will be destroyed. This means that we have to look at all the information we hold, and either be able to give a valid reason to keep it or destroy it.

Policy

To comply with GDPR and protect personal data, we will:

1. Make an initial review of the data we already have to sort out which is 'personal data' and which is 'non-personal data', whether it is held on paper or computer systems. GDPR only applies to personal data.
2. If a person cannot be identified from the data, then it will be called non-personal data, and the rules will not apply to it.
3. All personal data will be assessed to establish if it is also 'sensitive' data. Sensitive data is information which may reveal something about you that you may not want everyone to know, such as your sexuality, beliefs, any medical issues or disabilities, political views and issues from your past. Any sensitive personal data will be treated with greater security.

4. Any staff joining Forensic Defence after the 25th May 2018 will be required to sign to consent to their personal data being stored and processed in order to fulfil their contract of employment.
5. Director Mohammed QADERO is the designated DPO and should be contacted with any questions.
6. A data cleanse will occur on or around the 26th June annually, and a record will be made to evidence this.
7. Forensic Defence's GDPR policy will be accessible to all visitors to their website.
8. Two layers of verification have been applied for computer access.
9. All computers that store personal data are password protected and will time out automatically after 20 minutes.
10. All sensitive data is stored in an encrypted format and is password protected. Emails are sent using the Ministry of Justice secure CJSM system.
11. Hand written personal data will be stored in a locked room.
12. Hand written sensitive personal data will be stored in a locked drawer within a locked room.
13. All handwritten personal data will be shredded as soon as it has been stored electronically.
14. If our computers are lost or stolen, our IT provider is able to also create remote locking to add further security or conduct a 'data wipe' so that all information is deleted.
15. From 25th May 2018, all new suppliers and customers will be asked for their consent for us to gather, store and process their personal information. Consent will **not** be legal if it is gained via a pre-ticked box, or with only an 'OPT OUT' option. Under GDPR you must do something physical which means you have given your consent. This will include you putting a tick in a box, signing to say that you consent, or even telling someone that you consent.
16. Prior to 25th May 2018 we will only process your personal data if we can justify that it is in your best interests. If one of the six legal bases for doing this is not met, then we will destroy your data and record this.
17. Whether your personal data is held on paper or computer, you will be able to see it free of charge and request that we destroy it if required or give your consent that we can keep using it as we are.
18. You will still be able to 'unsubscribe' from our site. If we then contact you after you have unsubscribed, we will be breaching the GDPR.
19. We must tell everyone involved with us that we are complying with GDPR. This will be done by email, and our email signature will reflect this.
20. If we discover a data breach, we will report it to the ICO within 72 hours.

For any further information, please look at the Information Commissioners Office (ICO) on www.ico.org.uk

FORENSIC DEFENCE