GDPR TWO YEARS ON

Reza Nezam *reflects on the changes brought about by the General Data Protection Regulations and reveals there is still much work to be done*

It has been two years since GDPR was introduced in the UK and the EU to give people more control over their personal data and how it is used. Any company that stores or processes personal information about EU citizens within EU states must comply with GDPR, even if they do not have a business presence within the EU.

Law firm Gibson & Associates Solicitors conducted a survey of more than 1,000 people in the UK and Ireland to gauge whether the general public understand their rights under the legislation.

The results revealed that as many as one in five people have fallen victim to a data breach, while one in four are unaware as to whether they have had their personal data illegally accessed.

Of those who said that they had been the victim of a breach, only seven percent made a claim. When asked why they did not make a claim, 37 percent said they were not aware that they could do so, while 24 percent didn't think it was a big enough concern to bother trying.

Personal data breaches can include: access by an unauthorised third party; deliberate or accidental action (or inaction) by those responsible for your data; sending personal data to an incorrect recipient; computing devices containing personal data being lost or stolen; alteration of personal data without permission; or loss of availability of personal data.

GDPR places a duty on organisations to report data breaches within 72 hours of becoming aware of them

The GDPR places a duty on all organisations to report certain types of personal data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach. If a breach poses a high risk to individuals' rights, they must be informed without undue delay. Organisations are required to provide the following in clear and plain language: the nature of the personal data breach; the name and contact details of the organisation's data protection officer or another point of contact; a description of the likely consequences of the personal data breach; and a description of the measures taken, or proposed to be taken, to deal with the breach, including, where appropriate, measures taken to mitigate any possible adverse effects.

Any organisation that collects personal data has a legal duty of care to make sure every individual's information is protected. Anyone who has their data leaked due to the irresponsibility of a company is vulnerable to suffering financial losses. Regardless of how big or small these are, companies should be held accountable for their mistreatment of this often very sensitive data, which is why victims have the legal right to make a claim.

While it may not seem like a big deal to make a claim if you haven't suffered significant financial losses, individuals shouldn't be worried about whether they are going to have their personal information used without their knowledge. Making a claim isn't just about reimbursing the victim's financial loss, it can be used to recompense any emotional distress and ensure that the responsible organisation has suitable security methods in place to protect data against any future breaches.

Despite 80 percent of survey participants confirming they know what GDPR is , respondents showed significant gaps in knowledge when asked about the guidelines. Only 28 percent understood what personal information could be legally kept by an organisation, while 15 percent wrongly said that companies were not able to keep any personal data at all.

The full list of personal information that an organisation can keep on an individual under GDPR includes: your name; date of birth; address or mobile phone GPS; telephone number; an online identifier, such as IP address or email address; the job you do; your racial or ethnic origin; identification numbers, such as National Insurance and passport; items you view or buy online; your bank details, including credit cards; the school you went to; information on your health; biometric data, such as photos and fingerprints; details about your partner/family; membership of any Trade Union; religious or philosophical beliefs; political opinions; passwords; or details concerning your sex life and sexuality

There was also a significant lack of knowledge when respondents were asked what companies can legally do with personal data, with only 26 percent correctly identifying that organisations are able to do the following: use it to provide a service; make a recommendation; decide what you see online; directly sell to you; or sell the data to third parties. Some 14 percent incorrectly said that companies were not able to do any of the above with personal data.

GDPR was introduced to allow people to take back control of their personal information and make informed decisions about how it is used. While it falls to a company to responsibly handle someone's personal data, individuals need to be aware of what information is being stored about them and what can be done with it.

Despite 62 percent of respondents saying they do not trust companies to use their data responsibly, and 72 percent being greatly or somewhat concerned about organisations misusing their data, it is surprising to see that more than half (55 percent) of UK and Irish residents were not familiar with the means to request access to their data.

IF YOU ARE USING THE INTERNET OUTSIDE OF THE EU GDPR'S PROTECTION NO LONGER APPLIES

A subject access is a written or verbal request asking for access to personal information that an organisation holds or processes on you. You are able to make a subject access request (SAR) whenever you want to know about what personal data any company stores about you.

Following the changes made when GDPR was introduced, individuals can now make an SAR for free. If a request is considered to be "manifestly unfounded or excessive", a reasonable admin fee may be applied to a request. Using an SAR, individuals can request: a copy of their data; the reason why their data is being processed; what type of data is stored and processed; who receives the data; how long it is stored for; and how the data was collected.

To make a subject access request, you should find out which department and person you need to send the request to. Write to the organisation by recorded delivery or email, including your full name, address, contact telephone number, any account numbers, unique IDs and other information to distinguish who you are. You should also include specific details of the information you require and any relevant dates.

You may be charged an admin fee if your request isn't specific enough. For example, when making a request to see CCTV footage it would be reasonable to specify a location, date and time instead of asking for a month's worth of footage. In the request, you should also make reference to your right to make an SAR for free and the one-month deadline, which applies to the time period a company has to respond to a request. Finally, it is important to keep a copy of the SAR and any other correspondence. This will be useful if you need to make a complaint against an organisation that hasn't fulfilled a request.

An organisation is required to reply to an SAR within one month from the date it receives the request. This period can be extended by two months if a request is complex or there are multiple SARs made, but the company must get in touch during the first to explain why an extension is necessary. All

SARs must be completed free of charge; however, a reasonable fee can be requested if an SAR is unfounded or excessive, or additional copies of the personal data are requested.

Organisations should provide data in a commonly used electronic format unless this is not possible or it takes "disproportionate effort". Information should be provided in a concise, transparent and easily accessible form that is written in plain English and is capable of being understood by an average person.

GDPR WAS INTRODUCED TO ALLOW PEOPLE TO TAKE BACK CONTROL OF THEIR PERSONAL INFORMATION

Companies are allowed to withhold certain information if it could identify someone else and it is not reasonable to disclose that information. Also, if somebody making an SAR is being investigated for a crime or in connection with taxes and the investigation would be prejudiced if access to the data was granted.

GDPR is an EU law, which means that the benefits are focused on protecting the privacy of citizens of the European Union. Although some organisations have stated that they will roll out similar protections for users worldwide, currently, the legislation only applies to people who are browsing in the EU region.

This means that if you are outside of the EU, even temporarily, the same protections do not apply because websites determine the geographical location of their visitors based on their IP address. However, it is possible to change the IP address by using a VPN, meaning if you're travelling outside of the EU, you can still connect to an EU server and be treated as an EU citizen by websites.

To ensure you are protected under GDPR, you will need to sign up with a trusted VPN service; download the VPN and launch the application on your computer or mobile device; select a server to connect to – this can be anywhere across the globe, but will need to be in the EU in order to take advantage of GDPR protection; connect to a server in order to be assigned a new IP address; and then browse the internet at your leisure with added protections.

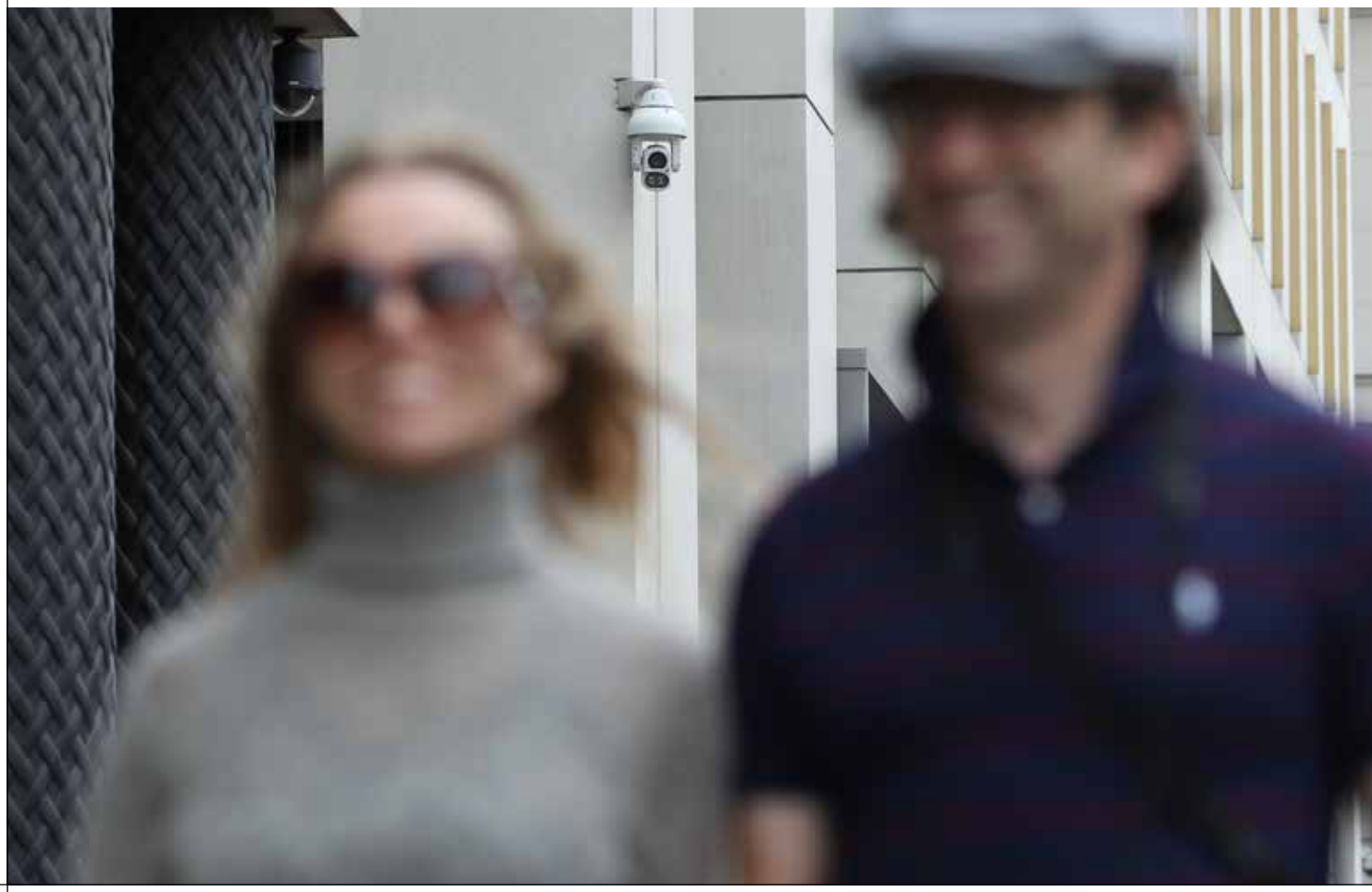
Using a VPN can also have numerous additional benefits, including encrypting your web connection and hiding your web traffic data. This means a VPN can provide protection by blocking websites and ISPs that collect your data.

In addition, you will also be able to browse websites that were previously blocked in a country outside of the EU. VPN tools are also considered to be extremely effective in keeping malware off mobile devices.

In the digital era, is it essential that data is protected. Misuse of data can result in discriminatory decisions, violation of privacy rights, identify theft, fraud, and much more. This is why you must be in control of your information. Now that the law has changed to strengthen what were once weak enforcement mechanisms, you have a responsibility to keep data secure and hold any organisations that infringe your rights to account ●

Reza Nezam is a data protection solicitor at Gibson & Associates, qualified as a solicitor in 2016 and has professional certification in data protection law.

When requesting CCTV footage it is prudent to provide details of specific location, date and time



Picture credit: Getty