GDPR & Privacy Policy 2018

23/05/2018

Bans Intruder & Fire Systems Ltd
Authored by: Jonathan Harrington

C:\Users\Harbans\Dropbox\banssec\GDPR Privacy Policy.docx

Contents

GDPR

What is GDPR?

The GDPR is Europe's new framework for data protection laws – it replaces the previous 1995 data protection directive, which current UK law is based upon. The EU's GDPR website says the legislation is designed to "harmonise" data privacy laws across Europe as well as give greater protection and rights to individuals. Within the GDPR there are large changes for the public as well as businesses and bodies that handle personal information, which we'll explain in more detail later.

After more than four years of discussion and negotiation, GDPR was adopted by both the European Parliament and the European Council in April 2016. The underpinning regulation and directive were published at the end of that month. After publication of GDPR in the EU Official Journal in May 2016, it will come into force on May 25, 2018. The two year preparation period has given businesses and public bodies covered by the regulation to prepare for the changes.

Both personal data and sensitive personal data are covered by GDPR. Personal data, a complex category of information, broadly means a piece of information that can be used to identify a person. This can be a name, address, IP address... you name it. Sensitive personal data encompasses genetic data, information about religious and political views, sexual orientation, and more.

These definitions are largely the same as those within current data protection laws and can relate to information that is collected through automated processes. Where GDPR differentiates from current data protection laws is that pseudonymised personal data can fall under the law – if it's possible that a person could be identified by a pseudonym.

So what is Different?

In the full text of GDPR there are 99 articles setting out the rights of individuals and obligations placed on organisations covered by the regulation. These include allowing

people to have easier access to the data companies hold about them, a new fines regime and a clear responsibility for organisations to obtain the consent of people they collect information about.

Companies covered by the GDPR will be more accountable for their handling of people's personal information. This can include having data protection policies, data protection impact assessments and having relevant documents on how data is processed. There's also a requirement for businesses to obtain consent to process data in some situations. When an organisation is relying on consent to lawfully use a person's information they have to clearly explain that consent is being given and there has to be a "positive opt-in".

Access to your Data

As well putting new obligations on the companies and organisations collecting personal data, the GDPR also gives individuals a lot more power to access the information that's held about them. At present a Subject Access Request (SAR) allows businesses and public bodies to charge £10 to be given what's held about them. Under the GDPR this is being scrapped and requests for personal information can be made free-of-charge. When someone asks a business for their data, they must stump up the information within one month. Everyone will have the right to get confirmation that an organisation has information about them, access to this information and any other supplementary information.
As well as this the GDPR bolsters a person's rights around automated processing of data. The ICO says individuals "have the right not to be subject to a decision" if it is automatic and it produces a significant effect on a person. There are certain exceptions but generally people must be provided with an explanation of a decision made about them.
The new regulation also gives individuals the power to get their personal data erased in some circumstances. This includes where it is no longer necessary for the purpose it was collected, if consent is withdrawn, there's no legitimate interest, and if it was unlawfully processed.

Our Data Processors

If you are using an alarm with 24-hour keyholder monitoring, then Southern Monitoring will be processing your data.
http://www.smon.co.uk/terms-and-conditions

Automated emails are handled by CampaignMonitor.
https://www.campaignmonitor.com/trust/gdpr-compliance/

Use of Personal Data - Customers

Personal Data we Hold

Name, Address, Email Address, Home/Work/Mobile telephone number

Notice and Consent for Use of Personal Data – Customers

What does the GDPR say?

Article 6(1)(b) gives Bans Intruder and Fire Systems Ltd a lawful basis for processing data where:

> "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"

To this end, our lawful consent for using our customer's data falls under these two categories

- Where Bans Intruder and Fire Systems Ltd has a contract with a customer and the processing of the customer's personal data is required to comply with their obligations under the contract.
- Where Bans Intruder and Fire Systems Ltd hasn't yet got a contract with the individual, but they have asked the company to do something as a first step (e.g. provide a quote) and their personal data requires processing on order to do what they ask.

Note: A contract does not have to be a formal signed document but can be a request for work to be carried out, such as in an emergency situation (e.g. to disable or repair a faulty intruder alarm).

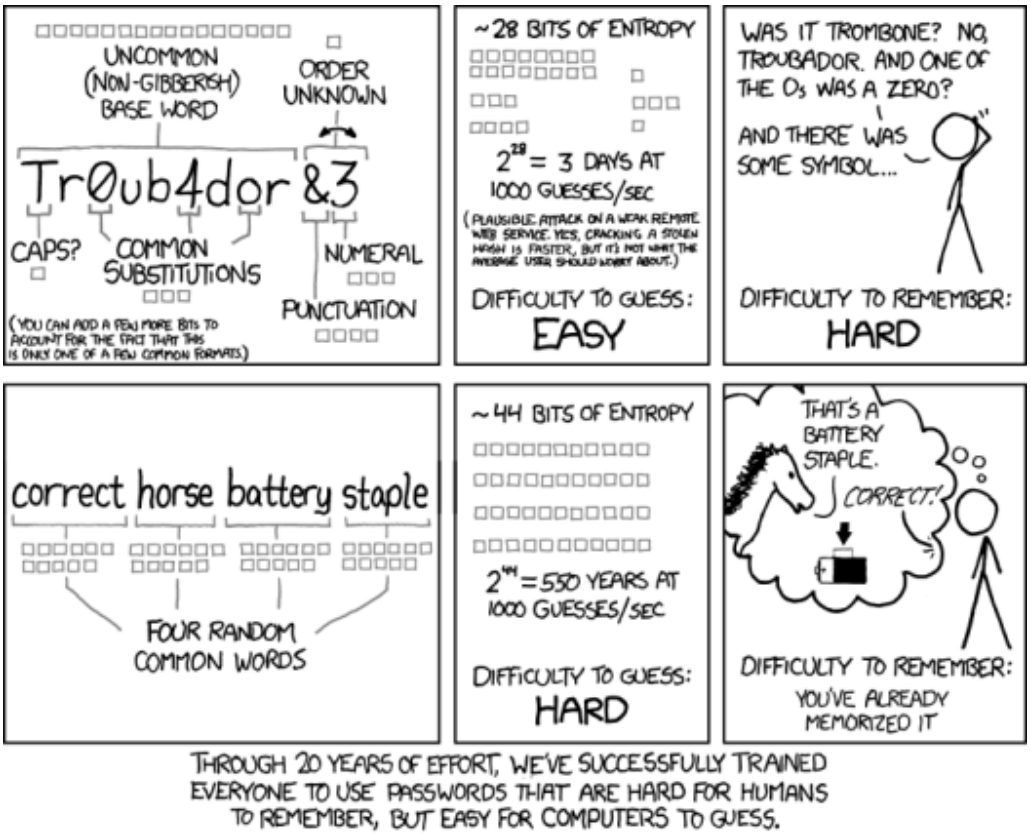
Customers have the right to access, to request deletion or restriction of processing of, and to correct any inaccuracies regarding their personal data held by Bans Intruder and Fire Systems Ltd.

Any inquiries sent via e-mail to:

DataProtectionOfficer.GB@BansSecurity.co.uk.

Best Practices for Employees

Password Policy



Example:
Banssecuritypassword1.
Long, mixed upper/lower case, includes numbers and punctuation

Storage

Paper copies of personal data are to be held in locked cabinets, and only those authorised should have access to the keys
Digital copies of personal data should be held on encrypted drives, that require passwords to decrypt.

Computers should log-off automatically when not in use, and require password to reinitialise.

Shredding

All unrequired paper documents containing personal data are to be **immediately** destroyed via shredding.

DNS

By default, DNS is usually slow and insecure. The ISP, and anyone else listening in on the Internet, can see every site visited and every app being used — even if their content is encrypted. Some DNS providers sell data about Internet activity or use it target advertising.

Company computers are to be set to use Cloudflare 1.1.1.1 DNS Servers.

Instructions for Windows

- Click on the Start menu, then click on Control Panel.
- Click on Network and Internet.
- Click on Change Adapter Settings.
- Right click on the Wi-Fi network you are connected to, then click Properties.
- Select Internet Protocol Version 4 (or Version 6 if desired).
- Click Properties.
- Write down any existing DNS server entries for future reference.
- Click “Use The Following DNS Server Addresses”.
- Replace those addresses with the 1.1.1.1 DNS addresses:
- For IPv4: 1.1.1.1 and 1.0.0.1
- For IPv6: 2606:4700:4700::1111 and 2606:4700:4700::1001
- Click OK, then Close.

Email

If in doubt, do not open an attachment. Email attachments are the easiest way for trojan or virus to enter the system.

Anti-Virus/Firewall

All company computers should be running Avast! Firewall and antivirus software. Spybot Search and Destroy from Safernetworking is to be used as a secondary line of defence against digital intrusion.

Data should be regularly backed up in line with the company's backup procedures.

Personal Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.

Use of Personal Data — Employees

Updated April 23, 2018

Upon becoming an employee of Bans Intruder and Fire Systems Ltd, a person acknowledges that Bans Intruder and Fire Systems Ltd, and similar cooperating organizations (contractors), lawfully use personal data in accordance with its legitimate commercial interests.

Personal data may include name, date of birth, gender, contact information, next-of-kin, work/education history. Medical data may also be taken where necessary to ensure the safe working of the employee, or of other employees.

As an NSI (National Security Inspectorate) registered company, all employees must be screened (10 years previous) for criminal convictions. Furthermore, financial checks are made [requirements specified within BS 7858:2012, audited by the National Security Inspectorate] which will check the following data.

- Adverse financial history: Identification of any County Court Judgments (CCJs), Court Decrees, Bankruptcy, Sequestration or Insolvency during the last 6 years. For CCJs and Court Decrees the report will also identify the actual amounts involved, court references, and whether the debts have been satisfied.
- Address history verification: Searches against the electoral register entries for the address provided returning the details found in the public register; searches in financial databases for active accounts to confirm the address provided.
- Linked addresses: Any other addresses found that are linked to the applicant's identity.
- Identity verifications: Searches to find matches on the name and date of birth for the address provided.
- Alias names: Searches for any alias names associated with the identity.
- Previous credit searches: Activity within the last 6 months such as applications for credit cards, loan applications and debt collection activity.
- Notices of any corrections: Identification of any corrections that the individual has applied to their credit file.

- HM Treasury and OFAC sanctions: Verification as to whether the individual has been listed for HM Treasury or OFAC sanctions.

Use of personal data may mean collecting, recording, organizing, structuring, and storing that data, as well as similar operations performed on that data.

The Data Protection Law in this country is:

General Data Protection Regulation (EU) 2016/679.

Personal data will be kept for an unspecified period of time for as long as the purposes stated above or other legitimate purposes apply.

Personal data may be sent, when necessary and appropriate, to any cooperating organization of Bans Intruder and Fire Systems Ltd.

Employees have the right to access, to request deletion or restriction of processing of, and to correct any inaccuracies regarding their personal data held by Bans Intruder and Fire Systems Ltd.

Any inquiries sent via e-mail to:

DataProtectionOfficer.GB@BansSecurity.co.uk.

NOTICE AND CONSENT FOR USE OF PERSONAL DATA - Employees

Upon becoming an employee of Bans Intruder and Fire Systems Ltd, I acknowledge that Bans Intruder and Fire Systems Ltd, and similar cooperating organizations (contractors), lawfully use my personal data in accordance with its legitimate commercial interests. I have been informed about and had the opportunity to read the Use of Personal Data page section within this document. I consent to the use of my personal data as stated within that section and as it may be amended from time to time.

Signature: _____

Print name: _____

Date: _____

Website Privacy Policy

What Are Cookies?

As is common practice with almost all professional websites our website uses cookies, which are tiny files that are downloaded to your computer, to improve your experience. This page describes what information they gather, how we use it and why we sometimes need to store these cookies. We will also share how you can prevent these cookies from being stored however this may downgrade or 'break' certain elements of the sites functionality.

How We Use Cookies

We use cookies for a variety of reasons detailed below. Unfortunately in most cases there are no industry standard options for disabling cookies without completely disabling the functionality and features they add to this site. It is recommended that you leave on all cookies if you are not sure whether you need them or not in case they are used to provide a service that you use.

Disabling Cookies

You can prevent the setting of cookies by adjusting the settings on your browser (see your browser Help for how to do this). Be aware that disabling cookies will affect the functionality of this and many other websites that you visit. Disabling cookies will usually result in also disabling certain functionality and features of the this site. Therefore it is recommended that you do not disable cookies.

Third Party Cookies

In some special cases we also use cookies provided by trusted third parties. The following section details which third party cookies you might encounter through this site.

This site uses Google Analytics which is one of the most widespread and trusted analytics solution on the web for helping us to understand how you use the site and ways that we can improve your experience. These cookies may track things such as how long you spend on the site and the pages that you visit so we can continue to produce engaging content.

For more information on Google Analytics cookies, see the official Google Analytics page.
Third party analytics are used to track and measure usage of this site so that we can continue to produce engaging content. These cookies may track things such as how long you spend on the site or pages you visit which helps us to understand how we can improve the site for you.
From time to time we test new features and make subtle changes to the way that the site is delivered. When we are still testing new features these cookies may be used to ensure that you receive a consistent experience whilst on the site whilst ensuring we understand which optimisations our users appreciate the most.
Our website uses the Google AdWords remarketing service to advertise on third party websites (including Google) to previous visitors to our site. Google Analytics remarketing will display relevant ads tailored to you based on what parts of the website you have been viewing. This does not in any way identify you or give access to your computer. Google Analytics remarketing allows us to tailor our marketing to better suit your needs and only display ads that are relevant to you.

You can opt out by downloading and installing this add-on for your web browser.
https://tools.google.com/dlpage/gaoptout/

A Note about CCTV

Using CCTV on your property

CCTV used on your property will be exempt from the Data Protection Act unless you are capturing footage of individuals outside your property.
However, regardless of whether your CCTV system is exempt, the ICO recommends that you use CCTV in a responsible way to protect the privacy of others.

1. Register with the Information Commissioner's Office as a CCTV operator
2. Have a stated purpose for your CCTV system and review this regularly
3. Carry out a Privacy Impact Assessment and publish this if appropriate
(You can find out more about Privacy Impact Assessments here.)
4. Put up clear signage, warning there is CCTV surveillance on the property
5. Publish the name of someone in your business that people can raise queries and complaints with
6. Appoint a person responsible for your CCTV system
7. Implement clear rules, policies, and procedures around CCTV surveillance for your business
8. Make sure your staff are fully aware of their responsibilities and any policies and procedures
9. Make sure CCTV recordings are captured and stored securely
10. Don't keep recordings for longer than you need (31 days is standard)
11. Delete older CCTV recordings regularly and in a secure way
12. Restrict staff access to CCTV recordings and implement a disclosure policy
14. Don't record conversations between members of the public
15. Follow recognised technical and operational standards as appropriate
16. Do not install CCTV in private spaces such as changing rooms and toilets
17. Make sure recordings you capture can be used by the police and courts if necessary, e.g. by ensuring the date and time are set correctly
18. Audit your CCTV operation regularly to check legal requirements, policies and standards are complied with
19. Publish your audit findings in a document

20. If you are using your CCTV system to cross-reference against a database (for example, if you are checking car number plates), then make sure your reference database is accurate and up to date.

Useful Links at the ICO

https://ico.org.uk/for-the-public/cctv-on-your-property/
https://ico.org.uk/for-organisations/register/
https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf