Hertfordshire Chamber of Commerce

All You Need to Know About

GDPR

With Guest Speakers:

ASHBOURNE INSURANCE

vwv

cribb CYBER SECURITY

www.hertschamber.com

GDPR: Key Legal Issues

Stephen Mcnamara
Consultant

vwv.co.uk | Offices in London, Watford, Bristol & Birmingham
Lawyers & Parliamentary Agents

Overarching principles

The GDPR introduces six general principles that apply to all processing of personal data. These are

- **lawfulness, fairness and transparency**
- purpose limitation
- data minimisation
- accuracy
- storage limitation (i.e. retention of personal data)
- integrity and confidentiality

The Seventh Principle = **Accountability**

Accountability

Transparency Notices

- Transparency is a key theme throughout GDPR
- The information that must be provided to individuals has increased considerably
- Must be in clear, concise, intelligible language and readily accessible. Think about how to communicate this to:

Staff

Contractors and suppliers

Individual Customers

Marketing Contacts

Staff of Corporate Customers

Event Attendees? (*What will we do with your data after today?)*

Transparency notice

- **Transparency notice** – A document (hardcopy or electronic), which may be made up of several smaller documents that will explain to individuals what personal information about them the business collects and how it will use that information.

  AKA : privacy notice; privacy policy; fair processing notices; fair collection statements

A good transparency notice?

Consent is changing

- Must have a lawful basis for processing personal data
- Many businesses have been using consent as the legal basis
- GDPR sets higher standard for consent: it must be freely-given, specific, informed, unambiguous and involve a clear affirmative action
- **Consent can be withdrawn at any time** – this includes those with whom data has been shared
- **Move away from consent as a legal basis for processing**

Other legal bases

Fear not: there are other legal bases that you can rely on:

- Necessary for performance of a contract
- Necessary for compliance with a legal obligation
- Legitimate interests
- Public interest
- Vital interest

Special categories of personal data? Stricter rules apply

Data processors (i)

- Familiar concepts of data controller and data processor continue but with important changes to role of data processor
- Certain GDPR responsibilities, obligations and penalties now apply directly to processors – significant shift of liability
- However: Stronger obligation on controllers to carry out thorough due diligence when selecting processors – must be satisfied can meet all GDPR requirements
- New rules will apply to existing contracts ⇨ review processor arrangements pre-May 2018
- IT support and cloud service providers – key risk as transfers outside the EEA are likely.

Data processors (ii)

- Written contract with processor remains compulsory and now more prescriptive list of obligations controllers must include:
  - Process only on controller's written instructions (including any processing outside EEA)
  - Use appropriate data security measures to same level as mandated for controllers
  - Ensure staff work under obligation of confidentiality
  - Assist controller with data subject rights e.g. subject access, right to erasure
  - Assist controller in compliance with data security obligations
  - Make relevant info available to controller and co-operate with audit
  - Use sub-processor only with controller's permission & flow down processing obligations

Data subjects' rights (i)

- Key aim of GDPR is to place individual at heart of data protection ⇨ data subjects' rights expanded and bolstered
- Organisations will need robust systems in place to enable e.g. erasure and restriction of processing to take place
- Working closely with data processors to comply with data subjects' rights will be necessary

Strengthening of individuals' rights

- Right to be informed
- Right of access + shorter Subject Access Request response limit
- Right to rectification
- Right to restrict processing
- Right to erasure
- Right to object
- Right to data portability
- The right not to be subject to automated decision-making (including profiling)

Breach notification

- Notification to ICO (and in certain cases the individuals) in event of a data breach
- Compulsory for 'serious breaches'
- Within 72 hours - sooner for major security breaches
- Likely to increase number of claims for civil damages
- Importance of having a robust process to identify security breaches, including arrangements with data processors, and to report to ICO

Stephen Mcnamara
Consultant
smcnamara@vwv.co.uk
0117 314 5449

cribb
CYBER SECURITY

Cyber Security is not just an IT issue, it is a boardroom and family issue

March 2018

by Bill Osborne MMS MBCI

cribb
CYBER SECURITY

CURRENTLY IT COSTS $380 PER RECORD PER DATA BREACH IT WILL BE A TOTAL COST OF $2 TRILLION BY 2019

November 2017

Credentials

cribb
CYBER SECURITY

Who am I?

cribb
CYBER SECURITY

- 40 years in IT – all areas
- Lectured for MoD Counter Intelligence (data security)
- Developed, created and provided successful services for Bank of England, Amazon, Healthcare (NHS and Private), Military, Insurance, SME's and small family companies… and many more

Laws & Regulation… but a few

Data Protection Act 1998

Current fine up to £500,000 – "FREE is too expensive"

Says EU……but yes we are sticking to this

GDPR
EU General Data Protection Regulation

Enforceable May 2018, the threat which has most people cold, FINES up to €20m or 4% of revenue – Tesco would have had a £1.94b fine!

The Information Commissioner's Office

- Teeth to fine
- 200 auditors being recruited
- Unannounced audit
- Public statements
- You need permission to hold PII – no mailshots etc.
- Data Destruction – simple threat (certs / “free” / method
- Abandoned paper files – threat
- Know where your data is
- See ICO web site for IG and other help

IASME / Cyber Essentials

- **Cyber Essentials – standard**
- **GDPR Readiness**
- **Cyber Essentials PLUS**
- **IASME GOVERNANCE** Cyber Essentials with GDPR Readiness
- Approved by GCHQ. Supported by HP, MOD, GCHQ, NCSC, NHS Wales, Solicitors Regulation Authority and more.
  - Only official certificate
  - FREE documents, FREE Cyber Insurance Possibly going to be mandated
  - Marketing badges
  - Differentiator (badge to use for marketing)
  - Proof of due diligence.

Personal Identifiable Information

- GDPR is to protect “PII” and make sure it is handled correctly
- Access
- Passwords
- Owner of the PII is the actual person. They can request ANYTHING (look, erase , change, forget, permission, …)

Case Studies

cribb
CYBER SECURITY

TESCO Bank

wonga.com

TalkTalk

"Case studies"

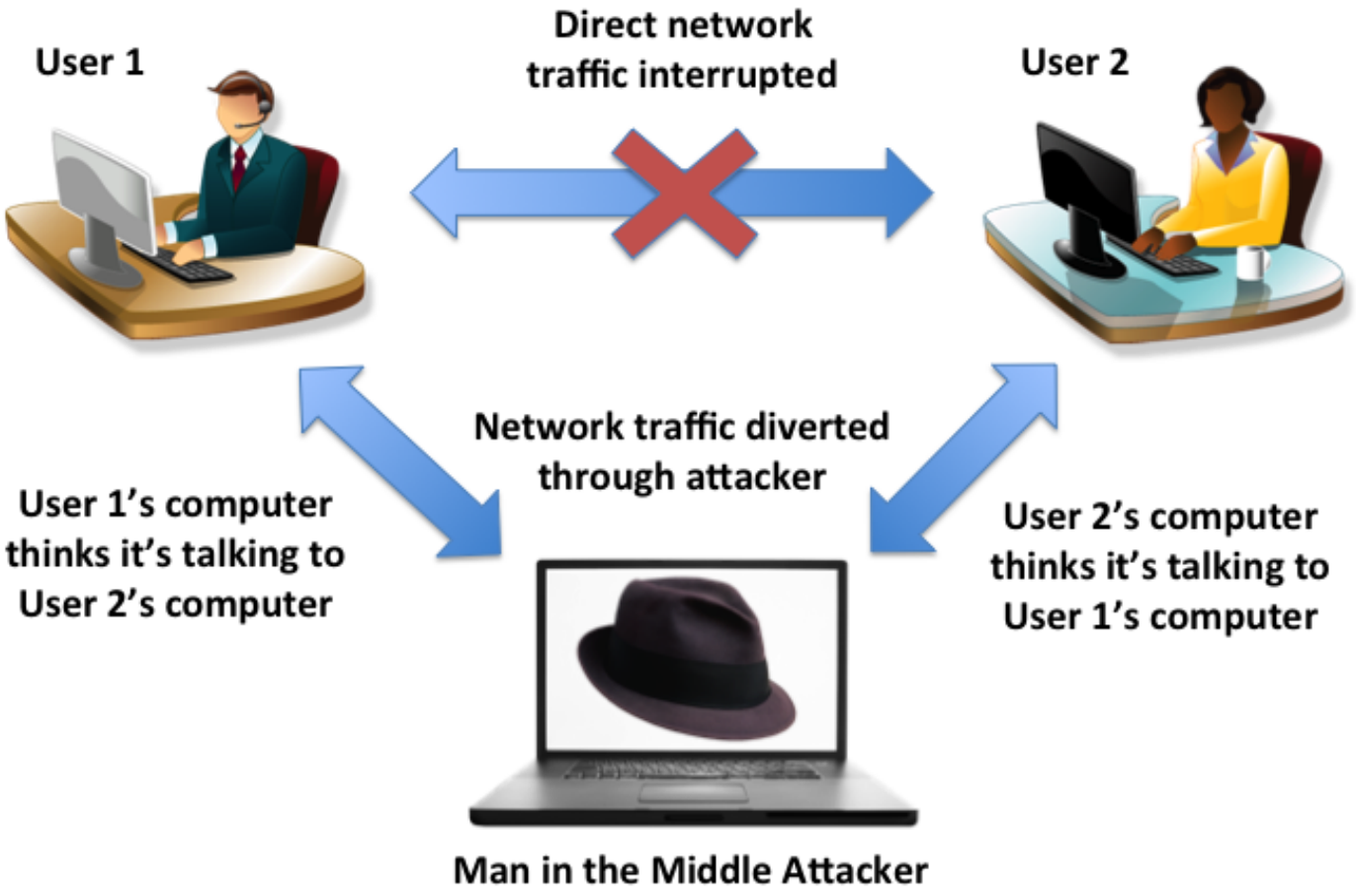
- TSA – recently Ransomware (bought for £80 with support desk) - 3 days plus, loss of business
- Vulnerability Scan revealed 1) data centre compromise 2) wasted money 3) security lapse
- Company - Phishing (£25,000)

- *NOTE: an external security company will provide an unbiased security review*

What do they want?

- MONEY
- Banned drugs
- Weakest link – photocopiers / printers?
- Research data
- Shut a manufacturing site or stop production?
- Personal data / payroll data of your staff
- Revenge
- Data for sale
- Because they can

Sample threat



Sample threat

- Virgin Media Scam on me
- My phone example – Amazon / Sky / Post Office inc. VIRUS attachments

Threats and Education

- Malware and viruses
- Social networking
- Physical security
- Protecting your kids online
- Dos
- Ransomeware
- IoT - the Internet of Things……FRIDGE access
- *Supply chain and customer pressure*
- 80% of used data bearing media or devices in the market (UK) STILL has data

Defensive Measures (just a few)

- **PCI DSS** – CHECK !!!!!!!!
- Timely patch updates
- Separated back ups
- Trusted partners
- Secure data destruction
- Intrusion Detection Systems (IDS)
- Health checks, risk assessments or audits, security policies (e.g. phishing attack)
- Find and fix weakest link – photocopiers (hard disks) / printers

Detection Services

- Readiness audit
- Vulnerability scan (passive)
- Data destruction audit
- Penetration testing (intrusive)
- Environment / physical

Prevention

- Get the issues identified and fixed
- Maintenance / support agreement (maintain your high standard) includes Status Reports, regular vulnerability scans, penetration testing, incident response plan
- More education (Portal)

SPECIAL OFFER to you

cribb
CYBER SECURITY

- **FREE WEBSITE** scan for threat and weaknesses
- Report issued to you
- External website Threat Analysis, to discover vulnerabilities of your website. This is with “deep dive” – this means a more comprehensive analysis, to find hidden pages and other unwanted elements. Vulnerabilities can allow someone to access your entire network, affect your insurance, reputation and marketing..

Thank you

WRO@Cribbcs.net 07702 766 119 www.cribcs.net

ASHBOURNE INSURANCE

Don't get lost in Cyber-space

Cyber & data liability

Cyber & data liability

Cyber insurance has been one of the fastest growing areas of the worldwide insurance market in recent years as a stream of high-profile data breaches and increasing regulatory pressures have combined to increase risk awareness.

ASHBOURNE INSURANCE

Cyber & data statistics

- Victims of cyber crime in the UK?
- **2.1 million annually**
- Fraud & cyber crime costs UK economy?
- **£11 billion annually**
- Cost of severe breaches to SMEs?
- **Average £310,000**
- Reported increases in security incidents?
- **22% year on year**

**department of skills & innovation 2015*

ASHBOURNE INSURANCE

Trends & challenges

- Immature market
- Failure to report
- Warranties & endorsements
- No consistency in cover
- Think data not cyber
- Yet another policy!

ASHBOURNE INSURANCE

Standard covers – "First party"

	Cover overview	Main areas
Breach costs	Costs incurred in responding to an actual or suspected date breach	• Legal fees • IT forensics • Notification costs • Credit monitoring • Call centre set-up
Cyber business interruption	BI following a cyber incident, including as a result of reputational damage	• Loss of income • Increased costs of working
Hacker damage	Costs incurred in replacing /repairing damage caused by hacker	• Computer systems • Computer programmes • Data held electronically
Cyber extortion	Costs incurred in the event of a threat to damage or disrupt computer systems, or publish information	• Ransom payment • Consultant to handle negotiation
Crises containment	Public relations response – prompt confident communication	• Expert advice to assist with developing communication strategies to running a 24/7 crises press office

Standard covers – "Third party"

	Cover Overview	Main Area
Privacy protection	Defence costs and awards/settlements made following legal action or investigation as a result of a data breach, invasion of privacy or breach of confidentiality	• Any breach of data protection act • Breach of confidence • Regulatory fines / awards • PCI charges • Claims by employees
Media liability	Defence costs and awards/settlements made following legal action as a result of a company's on-line presence	• Breach of Intellectual property • Defamation • Transmission of a virus

Optional policy covers

Add ons & extensions

- Cyber crime
- Telephone hacking
- Cyber hacktivism
- Financial crime
- Social engineering

ASHBOURNE INSURANCE

How much does it cost?

- Number of records
  - ✓ Including employees
- Sensitivity of data
- Trade sector
- Turnover
- Cyber security

ASHBOURNE INSURANCE

Red-button response

- First 48-hours are critical
- Cover is not a cash settlement
- Includes AD & MD breaches
- Emergency business recovery
- Protecting your reputation
- Legal obligations & defence costs

ASHBOURNE INSURANCE

Claims process

- **Incident**: data security breach occurs
- **Notify**: alert insurer immediately
- **Alert**: involve your incident response team
- **Investigate**: find out what happened
- **Stop**: prevent any further data loss
- **Assess**: potential consequences
- **Execute**: complete incident response plan
- **Evaluate**: how successful was the response

ASHBOURNE INSURANCE

Mind the Gap!

- Cyber / computer exclusions
- Digital world impacts on all businesses
- Excludes Fraud – financial crime
- Professional indemnity
- Cloud computing / outsourcing
- Little penetration within SME's

ASHBOURNE INSURANCE

Summary

- Think about loss of data
- Business interruption
- Employee errors
- GDPR implications
- Avoid “pop-up” products
- SME’s are a bigger target
- Engage with specialists

ASHBOURNE INSURANCE

Final thought…

- 1in 300 SME's will suffer a fire claim in 2018

Over 90% of SME's have cover in-place

- 1 in 8 SME's will suffer a data-breach

Under 2% of SME's have cover in-place

Statistics from the UK's largest insurer; Autumn 2017

ASHBOURNE INSURANCE

Questions?

ASHBOURNE INSURANCE

01992 471 001

https://www.ashbourneinsurance.co.uk/insurance-products/business/cyber-data-liability-insurance/

Hertfordshire Chamber of Commerce

Any Questions?

Our Guest Speakers:

VWV : Stephen Mcnamara

cribb CYBER SECURITY : William Osborne

ASHBOURNE INSURANCE : Peter Smits