UWE Bristol | University of the West of England

Presented by

Dr. Trupti Padiya

School of Computing and Creative Technologies

Advanced Databases UFCFU3-15-3

Personal Data Security and GDPR

Slides with modification adapted from Dr. Elias Pimenidis

Data and the World…

- A large part of our day is spent producing and consuming data!

- A lot of this data is personal – without even those that produce it and those that use it realising it.

- Data is being collected (by third parties), stored in places unknown to those it belongs to, shared with strangers, used by others, traded and displayed.

- Individuals often do all of the above with their data subconsciously

Personal data

What is Personal Data?

- Data elements that relates to an identified or identifiable individual.

- What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors.

- If you cannot directly identify an individual from that information, then you need to consider whether the individual is still identifiable.

Personal Data - 2

- Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and you may only process them in more limited circumstances.

- Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.

Personal data?

1. Which of the following is personal data?
   i. Name
   ii. Date of Birth
   iii. Place of Birth
   iv. Job title
   v. Office number
   vi. Mobile Phone Number
   vii. Mobile Phone Model
   viii. Email address
   ix. Bank card number

The role of data today

- Data & Personal data is not a new concept. It pre-existed computers and computer science.

- What has changed in the past few decades is the means by which new data is generated, the speed that data is produced at, the variety of means of storing it and the range of applications that can process it, transform it and share it.

- The ability to process, share it and store it online, beyond the control of the person it concerns, increases the risk and the impact of losing it. (cloud services)

- Big data – anonymity or Big Losses?

Even Governments can lose (your) data

https://www.theguardian.com/politics/2007/nov/21/immigrationpolicy.economy3

November 2007

The government was forced to admit the most fundamental breach of faith between the state and citizen yesterday when it disclosed that the personal records of 25 million individuals, including their dates of birth, addresses, bank accounts and national insurance numbers had been lost in the post, opening up the threat of mass identity fraud and theft from personal bank accounts.

Prime Minister Gordon Brown has said he "profoundly regrets" the loss of 25 million child benefit records. – 21 November 2007

http://news.bbc.co.uk/1/hi/7104945.stm

UK Law relevant to Data Protection

- Data Protection Act 1984 – world leader at the time

- Data Protection Act 1998 – refined the 1984 one and defined a more European dimension of the potential impact of loss of personal data. Conformed to the first European Directive on Data Protection

- GDPR – EU Regulation which was adapted as a UK law (2021). 2018

- Worldwide impact.

- Current Data Protection Act.

Data Protection Act 1998

- fairly and lawfully obtained;

- held only for specific and lawful purposes and not processed in any manner incompatible with those purposes;

- adequate, relevant and not excessive for those purposes;

- accurate and where necessary kept up-to-date, not kept for longer than necessary;

- processed in accordance with the rights of the person to whom the data refers;

- kept securely to ensure data is not lost, disposed of or misused;

- not transferred out of the European Economic Area unless the destination has an adequate level of data protection.

General Data

Protection Regulation

What is GDPR?

- The GDPR is Europe's new framework for data protection laws. It replaces the previous 1995 data protection directive.

- The new regulation started on 25 May 2018. It has been enforced by the Information Commissioner's Office (ICO).

- The Government has confirmed that the UK's departure from the European Union will not alter this.

GDPR Facts

GDPR in a Nutshell

Bigger Responsibility, Bigger Repercussions

Fines of up to 4% of turnover
Organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million.

Increased territorial scope
Applies to any company processing personal data of EU citizens, regardless of location.

Consent matters
Explicit consent must be provided in an intelligible and easily accessible form.

Right to access and portability
Users can inquire whether and how their personal data is being processed.

Breach notification within 72 hrs
Breaches must be reported within 72 hours of first having become aware of the breach.

Privacy by design
Data protection from the onset of the designing of systems, rather than a retrospective addition.

Right to be forgotten
Entitles the data subject to have the data controller erase his/ her personal data (and potentially third parties, too).

Mandatory data protection officers
Appointed in certain cases, to facilitate the company's need to demonstrate GDPR compliance.

GDPR LAWFULNESS PERSONAL DATA PROCESSING

Legal grounds and lawful basis - processing lawful if at least one of legal bases below

Consent

The consent of a data subject to the processing of his/her personal data

Legitimate interests

There is a weighed & balanced legitimate interest where processing is needed and the interest is not overridden by others

Public interest

Public authorities and organizations in the scope of public duties and interest

Contractual necessity

Processing is needed in order to enter into or perform a contract

Legal obligations

The controller is obliged to process personal data for a legal obligation

Vital interests

It is vital that specific data are processed for matters of life and death

Consent

Legitimate interests

Lawfulness of processing

Contractual necessity

Public interest

Vital interests

Legal obligations

Why is it important to the Computing World?

- Most data that we process is personal
- Most data that we store are captured from interactions with humans
- The way we process data can reveal very sensitive information about the personal life and the work of others.
- Vulnerable groups or communities can be exposed to risks
- Most of the SW that we build process data – often personal!

Securing Data?

- We often protect the environment that data is stored or processed – Antivirus software protecting networks and computer systems

- We protect the means by which we communicate data – encryption

- We protect data from physical destruction

- Do we protect data while we process it though?

- Do we use secure tools when processing data – when it is most vulnerable?

- The most vulnerable quality of data is integrity & at the same time is its most important one

The Easyjet data breach – April 2020

- **EasyJet** publicly announced the attack in May 2020. They told the BBC that they were only able to notify customers whose details were stolen in April 2020. **EasyJet** said "This **was** a highly sophisticated attacker. ... The affected data covers bookings made from 17 October 2019 to 4 March 2020.

- Pending law suit.

- Potentially huge business risk

You will find many other major incidents here:
https://en.wikipedia.org/wiki/List_of_security_hacking_incidents#2020s

BA – April to July 2018

- **More than 185,000 people may have had payment card details stolen in a hack attack on the BA website.**

- The victims were caught out by a website compromise that had gone undetected for months.

- BA only discovered the breach while investigating a breach of its website in September, which affected 380,000 transactions.

- BA owner IAG said both attacks seemed to have been carried out by the same group or gang. It added that it would contact the customers to let them know that their information had gone astray.

Sky routers with vulnerability - 2020

- Six million Sky routers had a serious security flaw.
- The problem has been fixed - but researchers say it took Sky 18 months to address.
- The vulnerability could have affected anyone who had not changed the router's default admin password.
- https://www.bbc.co.uk/news/technology-59332840#:~:text=About%20six%20million%20Sky%20routers,Sky%2018%20months%20to%20address.

Sky routers with vulnerability - 2020 (2)

- The flaw in software code would have allowed a hacker to reconfigure a home router, simply by directing the user to a malicious website via a phishing email.

- And then they could "take over someone's online life", stealing passwords for banking and other websites.

- Whether this whole issue could have rendered SKY responsible against the law, is very unclear.

Unsafe Routers could spell more personal trouble

- In early 2021 an insecure Vodafone router with a default password may have allowed a stranger to take over a couple's wi-fi and use it to upload illegal images of child abuse to the internet.

- The couple faced a police investigation that caused massive disruption to their lives and led to mental health problems.

Sharing your health records - NHS

- Information about your health and care helps the NHS to improve your individual care, speed up diagnosis, plan your local services and research new treatments.

- NHS Digital has a legal responsibility to collect data about NHS and social care services.

- The NHS cannot analyse all information on its own, so we safely and securely share some with researchers, analysts and organisations who are experts in making sense of complex information. We only share what's needed for each piece of research, and wherever possible, information is removed so that you cannot be identified.

- You can choose not to have information about you shared or used for any purpose beyond providing your own treatment or care.

- https://www.nhs.uk/using-the-nhs/about-the-nhs/sharing-your-health-records/

Managing your data choice

- From 25 May 2018 you can choose to stop your confidential patient information being used for purposes other than your own care and treatment. This choice is known as a national data opt-out. If you choose to opt out, NHS Digital will apply your opt-out from 25 May 2018. All other health and social care organisations are required to apply your opt-out by March 2020. Find out more about the <u>national data opt-out</u>.

- If you have previously registered an opt-out with your GP practice to request that NHS Digital does not use your confidential patient information (other than for your individual care and treatment), this will have automatically been converted to a national data opt-out on 25 May 2018. <u>Find out more about this conversion</u>.

- <u>https://www.nhs.uk/your-nhs-data-matters/</u>
  <u>http://content.digital.nhs.uk/yourinfo</u>

GDPR and UWE

- UWE has to adhere to the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018.
- https://www.uwe.ac.uk/about/structure-and-governance/data-protection/data-protection-statement-and-policy

- UWE Data Protection Policy
- https://www.uwe.ac.uk/study/it-services/information-security-toolkit/information-security-policies#section-3

Reference links

BA

- https://www.bbc.co.uk/news/technology-45953237
- https://www.bbc.co.uk/news/uk-england-london-45440850
- https://www.bbc.co.uk/news/technology-45446529
- https://www.bbc.co.uk/news/av/business-45446098

EASYJET

- https://www.bbc.co.uk/news/technology-52722626
- https://www.ft.com/content/7a1f3add-1882-4ff7-b5ec-e454aa16fd9a
- https://www.ncsc.gov.uk/news/easyjet-incident

HMRC

- https://www.computerweekly.com/news/2240084015/UK-government-loses-data-on-25-million-Britons
- https://www.theguardian.com/politics/2007/nov/21/immigrationpolicy.economy3
- http://news.bbc.co.uk/1/hi/7104945.stm

Further Reading on legislation

- https://ico.org.uk/your-data-matters/
- https://gdpr.eu/
- http://www.legislation.gov.uk/ukpga/1984/35/pdfs/ukpga_19840035_en.pdf
- http://www.legislation.gov.uk/ukpga/1998/29/contents
- http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted