Rural Femmes Intro

3rd of October 2021

RURAL FEMMES
ERASMUS+ PROGRAM

Data Protection & Online Safety - Overview

▶ Online Safety: In simple terms, *online safety* refers to the act of staying safe online. It is also commonly known as *internet safety*, e-safety and *cyber safety*

▶ Data Protection is: legal control over access to and use of data stored in computers

▶ *Privacy: Privacy as a right is difficult to define adequately. Privacy in the modern panoptic society must be flexible enough to address new technologies and developments and their privacy implications while at the same time certain enough to offer guidance and clarity as a matter of law. Keeping this tension in mind, it is extremely difficult to arrive at an appropriate definition. Description is therefore preferable"*

Both sides

- Think of it from a customer side of things are you experience it
- Think of it from running your own website/business

Social Media

Do you know how to use social media safely? True/False

▶ Be skeptical on social media – don't accept headlines at face

▶ Use security questions with answers that are discoverable from your profile

▶ Access social media from unsecured networks, eg hotel WiFi

▶ Close unused or obsolete social media accounts

Digital Media and Privacy

▶ Ultimate privacy in the digital and social media domain is very difficult because these media are designed for sharing information.

▶ The data we share online is and can be used by businesses to further their digital marketing agendas. For example, when we accept cookies on a website.

Cookies

Cookies

▶ A small file downloaded on to a user's computer/mobile device when user visits a website. The website then records the user's online activity

▶ Cookies can be used for targeted/personalised advertising

▶ The obligation is on the service provider to inform and seek consent from the user

▶ The user must 'opt in' explicitly or implicitly

▶ Reference to cookies in a website's terms and conditions is not sufficient

▶ If you have enabled your browser's 'Do Not Track' setting, then cookies will initially be disabled by default

Location Data

▶ Where processing of data allows geographical location of user to be identified – a value added service

▶ Use in marketing activities

▶ E-Privacy Regulations 2011– must be either anonymous or with consent of the user

▶ Must be informed consent

▶ It must be possible for user to withdraw consent

▶ Location data can only be used for purpose of providing the 'value added' service – to which the user has consented

Spam

- Unsolicited bulk commercial emails

- Often, spam email is sent for commercial purposes. While some people view it as unethical, many businesses still use spam

- The cost per email is incredibly low, and businesses can send out mass quantities consistently. Spam email can also be a malicious attempt to gain access to your computer

- **Types of Spam: Commercial advertisements, antivirus warnings, email spoofing, sweepstakes winners, money scams**

Data Protection

▶ **Data Protection relates to the way in which organisations deal with personal information**

▶ Data Protection Acts 1988 and 2003

▶ General Data Protection Regulation 2016

▶ Data Protection Act 2018

Data Protection

▶ Large amounts of data about individuals can be collected, stored and transferred via computers

▶ Risk of misuse and unauthorised access

▶ The aim of data protection laws is to balance the right of organisations to gather data and the right of individuals to control the content and use of such data.

Who is protected?

▶ Data subjects and their personal data

▶ Data subject – an individual who is the subject of personal data

▶ Personal data – data relating to a living individual who is or can be identified by the data or from the data in conjunction with other information that is in or is likely to come in to the possession of the data controller

Rights of Data Subjects under GDPR

- Right to be informed

- Right to access information

- Right to rectification

- Right to erasure

- Right to data portability

- Right to object

- Right of restriction

- Rights related to automated decision making

- Special Protections for Children

- Digital age of consent

- Child for the purposes of GDPR

- Offence in relation to processing data of a child for marketing purposes

- Right to be forgotten for children

- Codes of Conduct for data processing and children

EU Data Protection

▶ A right 'to be forgotten'. You will be able to ask to delete your personal data if you no longer want it to be processed, and there is no legitimate reason for a company to keep it (Art. 17 of the Regulation)

▶ In cases when companies need your consent to process your data, they will have to ask you for it and clearly indicate what use will be made of your personal data (Art. 4 (11) and 7 of the Regulation)

▶ If your data is lost or stolen, and if this data breach could harm you, the company causing the data breach will have to inform you (Art. 33-34 of the Regulation)

▶ Better protection of children online. Any information addressed specifically to a child will need to be adapted to be easily accessible, using clear and plain language. (Art. 8 of the Regulation)

Sensitive Personal Data – Additional Protection

▶ the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject

▶ whether the data subject is a member of a trade union

▶ the physical or mental health or condition of the data subject

▶ the commission or alleged commission of any offence by the data subject, or

▶ any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings

Co-funded by the
Erasmus+ Programme
of the European Union

Data Protection and Direct Marketing post GDPR

▶ Targeted direct marketing is still a legitimate activity

▶ The basic rule that applies to direct marketing is that you need the consent of the individual to use their personal data for direct marketing purposes. As a minimum, an individual must be given a right to refuse such use of their personal data both at the time the data is collected (an "opt-out") and, in the case of direct marketing by electronic means, on every subsequent marketing message. The "opt-out" right must be free of charge.

▶ You must also make clear who you are and where you obtained the individual's personal data (where this is not obvious).

Offences and Penalties

▶ The EU General Data Protection Regulation (GDPR) has attracted media and business interest because of the increased administrative fines for non-compliance.

▶ **There are two tiers of administrative fines that can be levied as penalties for non-compliance:**

▶ Up to €10 million, or 2% annual global turnover – whichever is higher.

▶ Up to €20 million, or 4% annual global turnover – whichever is higher.

▶ The fines are based on the specific articles of the Regulation that the organisation has breached and calculated in the total worldwide annual turnover of the preceding financial year.

▶ Infringements of the organisation's obligations, including reporting of data security breaches, will be subject to the lower level, whereas infringements of an individual's privacy rights will be subject to the higher level.

▶ **Souce: itgovernance.eu, 2020**

Co-funded by the
Erasmus+ Programme
of the European Union

Offences and Penalties

▶ However, not all GDPR infringements lead to data protection fines. Supervisory authorities such as the Data Protection Commission (DPC) in Ireland has a range of corrective powers and sanctions to enforce the GDPR. These include:

▶ Issuing warnings and reprimands;

▶ Imposing a temporary or permanent ban on data processing;

▶ Ordering the rectification, restriction or erasure of data, and;

▶ Suspending data transfers to third countries.

▶ In addition, data subjects have a right to take legal proceedings against a controller or a processor if he or she believes that his or her rights under GDPR have been infringed.

▶ **Souce: itgovernance.eu, 2020**

Ways to keep your personal information safe online

▶ **Think before you click**

▶ **Use Strong Passwords**

▶ **Verify website safety**

▶ **Use anti-virus and internet security software**

Password Security

▶ **Good practice**

• Use at least eight characters and a combination of upper and lower case letters, numbers and keyboard symbols such as !&*.

• Never disclose your password to anyone else.

• Don't enter your password when others can see what you are typing.

▶ **Bad Practice**

• Use the same strong password for multiple accounts – if one account is hacked, then all of your accounts are compromised.

• Use your favourite sports team or band.

• Refer to hobbies, interests, pets or family, especially if you talk about these on social media.

• Words from the dictionary, or letters consecutively shown on the keyboard, eg ASDFG or 12345

Password Security

▶ Use a password manager

▶ Multi-factor authentication

▶ Biometrics

Password Security

► https://passwords.google.com/ - turn this on in the settings

► Memorizing passwords is hard

► Free

► Saves and autofills passwords as well as credit card numbers and addresses

► Accessible across every device that supports Google Chrome

► Only available using Google Chrome

► Paid password management systems e.g. Bitwarden

Data breaches

► Data (or information) breaches can happen in many ways. Information storing equipment could be lost, stolen, damaged, or the equipment could break down. Human error could be involved (eg emailing the wrong person accidently) or even deliberate human action (eg sharing confidential data on purpose).

► Data can be targeted by cyber criminals in a cyber attack. A cyber attack is when someone illegally attempts to bypass the security or integrity of a device or network belonging to an individual or organisation. Cyber criminals aim to:

  ► damage or obtain and exploit information

  ► harass, embarrass or slander individuals or organisations

  ► steal money or demand ransoms

Types of Cyber Crime

- Hacking
- Theft
- Identity Theft
- Malware
- Breach of Copyright
- Types of cyber crime
  - Cyberbullying
  - Child soliciting

Why cyber security is important

▶ Has serious negative consequences for organisations and individuals

▶ For individuals, becoming a victim could mean financial damage, disruption to their daily lives, and short and long term emotional and psychological effects.

Successful cyber attacks

► Tricked by hackers

► Passwords

► Phishing email

Social engineering and phishing

- appealing to a person's desire to get a good deal or to help others
- creating a sense of urgency or fear

Smishing and vishing