Privacy and Data Protection in the Remote Working World

Webinar on 21 April 2020

John Popolizio,CEO Sovy

GRIFFITH COLLEGE

iSME
Irish SME Association

Online Workshop Series
"Restart Your Business,
Rethink Your Strategy"
In Response to COVID-19

sovy

Bonus Webinar

Privacy and Data Protection in the Remote Working World

- This workshop addresses privacy, conduct and data protection essentials for businesses facing new challenges with global remote working and preparing to return to on-site operations
- While many organisations have enabled privacy compliance programmes to meet General Data Protection Regulation (GDPR) requirements, many are still on the journey
- The thrust into global remote working has posed new challenges, some of which must be handled by strengthening privacy, employee conduct, data protection policies and procedures
- We will explore those changes, discuss practical options to implement improvements and answer question from the group
- Also, we will review recent regulator guidance and court decisions that will require even more changes this year and next for all businesses for both their physical and digital operations

GRIFFITH COLLEGE

iSME

Irish SME Association

Online Workshop Series
"Restart Your Business, Rethink Your Strategy"
In Response to COVID-19

sovy

Housekeeping

This webinar is educational!

https://www.linkedin.com/in/johnpopolizio/

- ❑ John Popolizio (JP) is your presenter and Michael Bosonnet is your moderator

  About JP
  - ✓ 35 years in technology, risk, compliance and security
  - ✓ Been involved in cool stuff (Citibanking, ePayments, early Cyber)
  - ✓ Passionate about helping SMEs navigate complex compliance
  - ✓ Co-founded Sovy to simplify business compliance with affordable online compliance as a service for privacy, conduct and anti-fraud

- ❑ **I can** offer insight based on experience
- ❑ **I am not** an attorney and so my insight is not legal advice
- ❑ **I cannot** speak for the regulators; and they might not agree with my interpretations

- ❑ This webinar and its materials reference publicly available information
- ❑ Sources and copyrights are noted
- ❑ References to companies and their products are not commercial endorsements

GRIFFITH COLLEGE

iSME Irish SME Association

SOVY

Increasingly Complex Rules of Trade

Global Remote Working Conditions

Cloud Services

Privacy and Data Protection in the Remote Working World

Online Workshop Series "Restart Your Business, Rethink Your Strategy" In Response to COVID-19

GRIFFITH COLLEGE

ISME
Irish SME Association

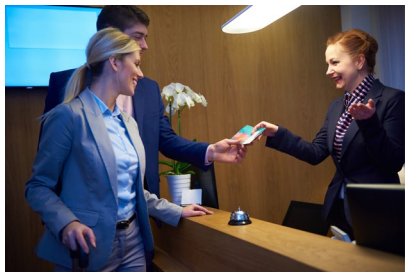
SOVY

SMEs Must Comply to Strict Laws

Privacy, Conduct, Anti-Fraud & Employment

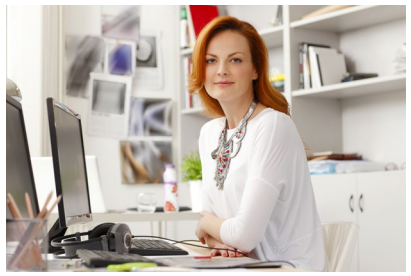
Family-Run Businesses

Part of a Supply Chain



Subsidiaries and Franchises

High-Turnover Workforce



Sole Traders and Work-at-Home

Privacy and Data Protection in the Remote Working World

Online Workshop Series "Restart Your Business, Rethink Your Strategy" In Response to COVID-19

GRIFFITH COLLEGE

iSME Irish SME Association

SOVY

GDPRvisual

Global Scope

Any EU business

Any business that offers goods and services within EU

Who

Data subjects (people)

Data controller

Data processor

HubSpot

Supervisory Authorities

Examples

An Coimisiún um Chosaint Sonraí
Data Protection Commission

ico.
Information Commissioner's Office

Personal Data

Name | Address | Email | IP| Mobile | Location Data | Image

Consent

Freely given, informed, unambiguous

Sometimes must be explicit

Privacy Rights

Transparency to be Informed | Access | Rectification | Erasure | Restrict or Object to Processing | Automated Decision Making & Profiling | Data Portability | Lodge a Complaint

The Lawful 6

Collect and process with

1. Consent
2. Performance of Contract
3. Compliance with a Legal Obligation
4. Legitimate Interests
5. Protecting a Person's Vital Interests
6. Performing a Task in the Public Interest

Identity

Identified vs Identifiable

Compliance Programme

Awareness | Policy | Training | DPO or Point Person | Data Handling Assessments | Record of Data Processing | Privacy Risks | Privacy by Design | DPIAs & LIAs | Procedures | Security | Testing & Evidence | Rights Management | Breach Detection, Response & Notifications

Processing

Collecting | Manipulating | Storing | Transmitting | Disclosing | Erasing

Special Category Sensitive Data

Requires Extra Care | Explicit Consent

Religion | Beliefs

Biometrics

Genetic

Health

Political View

Race | Ethnicity

Sex Life | Sexual Orientation

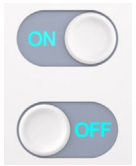
Trade Union Membership

Third Parties

Directed by Controller

Data Processing Agreement

Cookies & Banners



International Data Transfers

Countries designated having adequate levels of data protection

Binding corporate rules | Model contract clauses

Privacy shield

Data Management

Credits: Licensed Adobe Stock; Corporate and Agency Icons; APA Image

SOVY ACADEMY

6 Things for Understanding the Life-cycle of the Personal Data You Handle

Credits: GDPR Awareness Coalition

Privacy and Data Protection in the Remote Working World

Online Workshop Series
"Restart Your Business, Rethink Your Strategy"
In Response to COVID-19

GRIFFITH COLLEGE

iSME
Irish SME Association

SOVY

Some Important Tasks

Focus on Understanding Data Handling

- ❑ Find and Record, then Analyse
  - ✓ Understand where and how data travels
- ❑ Reduce or Remove
  - ✓ Have retention / deletion rules
- ❑ Notify Data Subjects
  - ✓ Privacy Notices, tell people their rights
- ❑ Ensure suppliers follow the rules
  - ✓ Processing Agreements, supplier investigation
- ❑ Respond and report
  - ✓ Look out for breaches, data requests, unsafe systems
- ❑ Design-in Privacy
  - ✓ All new processes should be examined for privacy-safety (DPIA)
  - ✓ Record the Legitimate Interests Analysis tests: Purpose | Necessity | Balancing

Privacy and Data Protection in the Remote Working World

Online Workshop Series
"Restart Your Business, Rethink Your Strategy"
In Response to COVID-19

GRIFFITH COLLEGE

iSME
Irish SME Association

SOVY

Privacy and Data Protection in the Remote Working World

Online Workshop Series "Restart Your Business, Rethink Your Strategy" In Response to COVID-19

GRIFFITH COLLEGE

ISME
Irish SME Association

SOVY

Hotel Fined For Breakfast List Data Breach

JULY 9, 2019 BY BEN (LUCKY) 27

In the past couple of days I've written about how both **British Airways** and **Marriott** are facing nine figure fines for GDPR violations related to their data breaches. These fines can be up to 4% of a company's annual revenue, so the fines have the potential to be massive.

While not nearly as big, **@Dailybits** and **@fotograaf** point to another very interesting hotel data breach. This time we're not talking about a fine of tens of millions of GBP, and we're not talking about something that impacted tens of millions of people.

Rather we're talking about a hotel breakfast. **The GDPR enforcement tracker** shows **a July 2 fine against the World Trade Center Bucharest (which has a Pullman hotel) in the amount of 15,000 Euros**. The breach? **A list containing the names of 46 guests who were entitled to breakfast at the hotel was photographed by an unauthorized party**. Here's the summary of the incident:

> *The breach of data security was that a printed paper list used to check breakfast customers and containing personal data of 46 clients who stayed at the hotel's WORLD TRADE CENTER BUCHAREST SA was photographed by unauthorized people outside the company, which led to the disclosure of the personal data of some clients through online publication. The operator of WORLD TRADE CENTER BUCHAREST SA has been sanctioned because it has not taken steps to ensure that data is not disclosed to unauthorized parties.*

It's said that the hotel didn't implement adequate technical and organizational measures to ensure a level of security that's appropriate.

Credits: https://onemileatatime.com/hotel-breakfast-list-data-breach/

Privacy and Data Protection in the Remote Working World

Online Workshop Series "Restart Your Business, Rethink Your Strategy" In Response to COVID-19

GRIFFITH COLLEGE

iSME
Irish SME Association

SOVY

Privacy and Data Protection

Personnel Management

Credits: KTT

Privacy and Data Protection in the Remote Working World

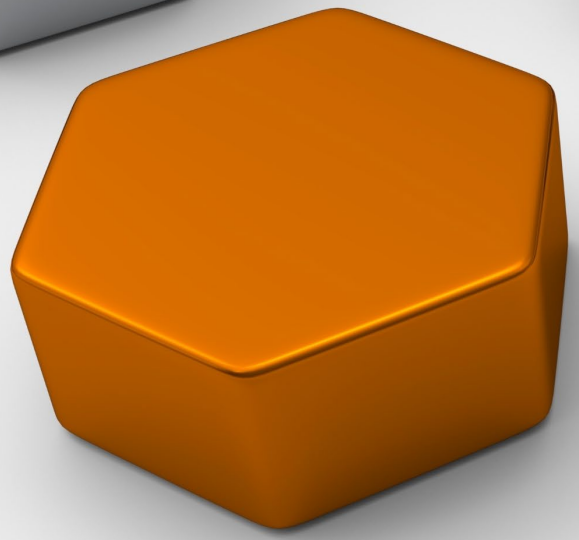
Online Workshop Series
"Restart Your Business, Rethink Your Strategy"
In Response to COVID-19

GRIFFITH COLLEGE

iSME
Irish SME Association

sovy

Continual Compliance Commitment



Assessment

Policy

Training

Operational Practice

Evidence of Compliance

Privacy and Data Protection in the Remote Working World

Online Workshop Series
"Restart Your Business, Rethink Your Strategy"
In Response to COVID-19

GRIFFITH COLLEGE

ISME
Irish SME Association

SOVY ACADEMY

Working Remotely

Tips for You and Your Staff

1. Follow your organisation's policies, procedures and guidance

- Your organisation will have adapted their approach to ensure that data is adequately protected.
- Avoid the temptation to do things in a way you think is more convenient, such as sending emails through your personal account or using video conferencing apps you use with friends for work calls.

2. Only use approved technology for handling personal data

- If your organisation has provided you with technology such as hardware or software you should use it. This will provide the best protection for personal data.

3. Consider confidentiality when holding conversations or using a screen

- You may be sharing your home working space with other family members or friends. Try to hold conversations, where they are less likely to overhear you and position your screen where it is less likely to be overseen.

4. Take care with print outs

- At the office, it is likely you can use confidential waste bins. At home you won't have that facility. Follow your organisation's guidance or safely store print outs until you can take them into the office and dispose of them securely.

Credits: ICO guidance

Privacy and Data Protection in the Remote Working World

Online Workshop Series
"Restart Your Business, Rethink Your Strategy"
In Response to COVID-19

GRIFFITH COLLEGE

ISME
Irish SME Association

SOVY

Working Remotely

Tips for You and Your Staff

5. Don't mix your organisation's data with your own personal data

- If you have to work using your own device and software, keep your organisation's data separate to avoid accidentally keeping hold of data for longer than is necessary. Ideally, your organisation should have provided you with secure technology to work with.

6. Lock it away where possible

- To avoid loss or theft of personal data, put print outs and devices away at the end of the working day if possible.

7. Be extra vigilant about opening web links and attachments in emails or other messages

- Don't click on unfamiliar web links or attachments claiming to give you important COVID-19 updates. We're seeing a rise in scams so follow guidance such as National Cyber Security Centre's (NCSC) guidance on spotting suspicious emails.

Credits: ICO guidance

Privacy and Data Protection in the Remote Working World

Online Workshop Series
"Restart Your Business, Rethink Your Strategy"
In Response to COVID-19

iSME
Irish SME Association

Working Remotely

Tips for You and Your Staff

8. Use strong passwords

- Whether using online storage, a laptop or some other technology, it's important to make your passwords hard to guess. The NCSC recommends using three random words together as a password (eg 'coffeetrainfish' or 'walltincake'). Make sure you use different passwords for different services too. See discussion on strong passwords…

9. Communicate securely

- Use the communication facilities provided to you by your organisation where available. If you need to share data with others then choose a secure messaging app or online document sharing system. If you have to use email, which isn't always secure, consider password protecting documents and sharing the passwords via a different channel, like text.

10. Keep software up to date

- If you're using your own equipment, don't be an easy target for hackers. Keep your security software up to date to make it more difficult for them to get in. If your organisation has provided you with technology to work from home, this should be managed for you.

Credits: ICO guidance

Privacy and Data Protection in the Remote Working World

Online Workshop Series
"Restart Your Business, Rethink Your Strategy"
In Response to COVID-19

GRIFFITH COLLEGE

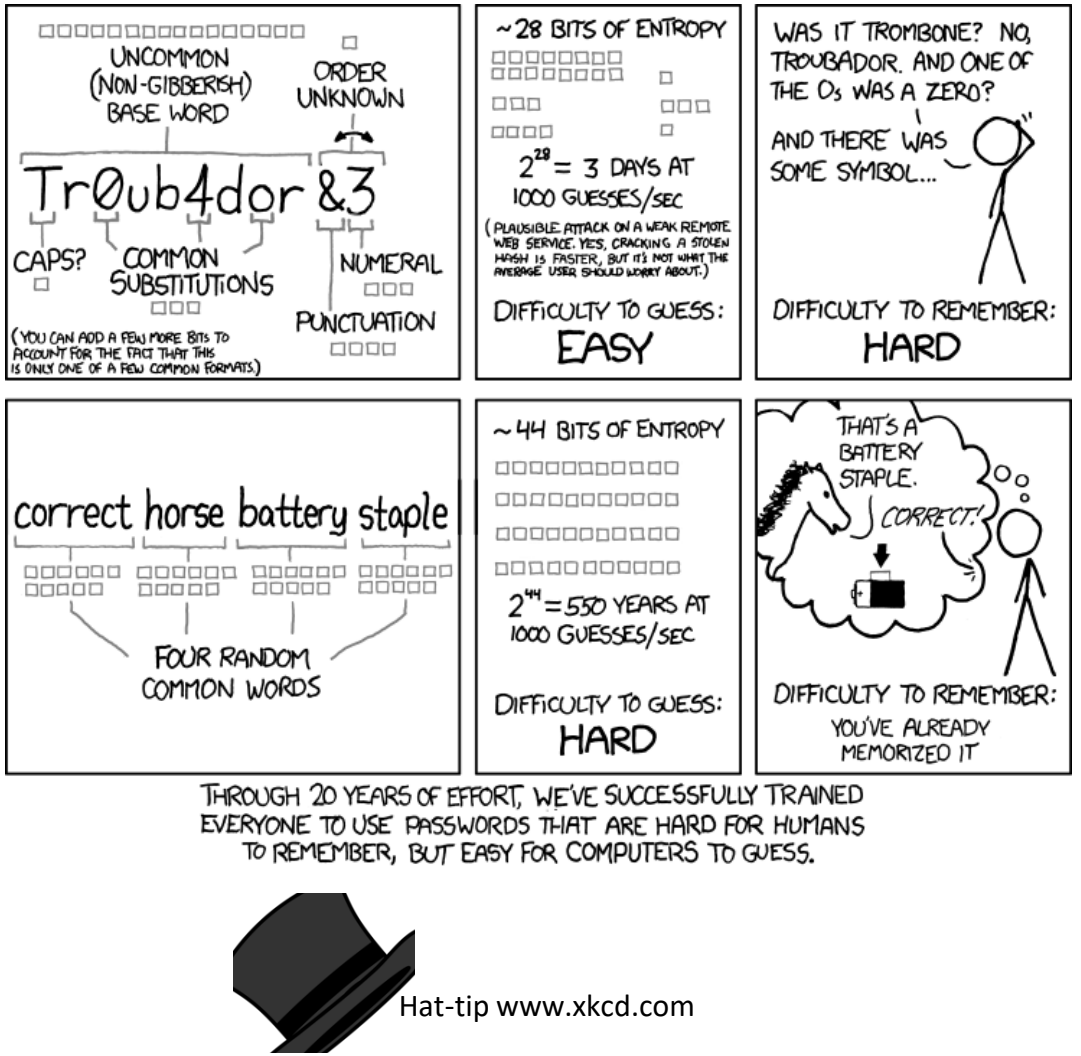
ISME
Irish SME Association

SOVY

Working Remotely

Making Strong Passwords

- ❑ **When the rules allow, combine the following:**
  - Symbols (e.g., ! @ # $ % & * { } < >)
  - Numbers (e.g., 0 1 2 3 4 5 6 7 8 9)
  - Lowercase Characters (e.g., a b c d e f g h)
  - Uppercase Characters (e.g., A B C D E F G H)
- ❑ **Avoid using similar characters in sequence:**
  - Example: do not combine i, l or 1
  - Example: do not combine o, 0 or O
- ❑ **Avoid substituting symbols or numbers for letters:**
  - Example: do not substitute $ for S
  - Example: do not substitute 3 for E
- ❑ **Add numbers or symbols in between the letters of a word instead of always at the beginning or the end of the word**



Hat-tip www.xkcd.com

Credits: xkcd.com

Privacy and Data Protection in the Remote Working World

Online Workshop Series
"Restart Your Business, Rethink Your Strategy"
In Response to COVID-19

GRIFFITH COLLEGE

ISME
Irish SME Association

SOVY

Working Remotely
Heightened Risks

1. **Secure Connections**.
- Companies should make remote access as secure as possible under the circumstances.
- This includes the use of Multi-Factor Authentication and secure VPN connections that will encrypt all data in transit.

2. **Company-Issued Devices.**
- As new devices such as computers and phones are acquired or repurposed for remote working, ensure that they are properly secured.
- This includes locking down the devices so applications cannot be added or deleted by the user, and installing appropriate security software (such as Endpoint Detection & Response and Mobile Device Management)

3. **Bring Your Own Device (BYOD) Expansion.**
- Be aware of the security risks and consider mitigating steps.
- Some personal devices are not properly secured or are already compromised.
- Malware should be required.

Credits: NYS Finance

Privacy and Data Protection in the Remote Working World

Online Workshop Series
"Restart Your Business, Rethink Your Strategy"
In Response to COVID-19

GRIFFITH COLLEGE

iSME
Irish SME Association

SOVY

Working Remotely
Heightened Risks

4. Remote Working Communications.

- Remote working has increased reliance on video and audio-conferencing applications, but these tools are increasingly targeted by cybercriminals.
- Configure these tools to limit unauthorized access, and make sure that employees are given guidance on how to use them securely.

5. Data Loss Prevention.

- Employees may be using unauthorized personal accounts and applications, such as email accounts, to remain productive while remote working.
- Remind staff not to send Nonpublic Information to personal email accounts and devices.
    - Anticipating and solving productivity problems will reduce the temptation to use such devices.

Credits: NYS Finance

Privacy and Data Protection in the Remote Working World

Online Workshop Series
"Restart Your Business, Rethink Your Strategy"
In Response to COVID-19

iSME
Irish SME Association

Working Remotely
Additional Risks

Increased Phishing and Fraud

- There has been a significant increase in online fraud and phishing attempts related to COVID-19.
- For example, in the United States, the FBI has reported that criminals are using fake emails that pretend to be from the Centers for Disease Control and Prevention (“CDC”), ask for charitable contributions, or offer COVID-19 relief such as government checks.
- Remind your staff to be alert for phishing and fraud emails
- Revisit phishing training and testing at the earliest practical opportunity.
- Now that face-to-face work is curtailed, authentication protocols may need to be updated – especially for key actions, like security exceptions and wire transfers.

Third-Party Risk

- The challenges created by the COVID-19 pandemic have also affected third-party vendors, re-evaluate the risks to your critical supply vendors

Credits: NYS Finance

Privacy and Data Protection in the Remote Working World

Online Workshop Series
“Restart Your Business, Rethink Your Strategy”
In Response to COVID-19

GRIFFITH COLLEGE

iSME
Irish SME Association

SOVY

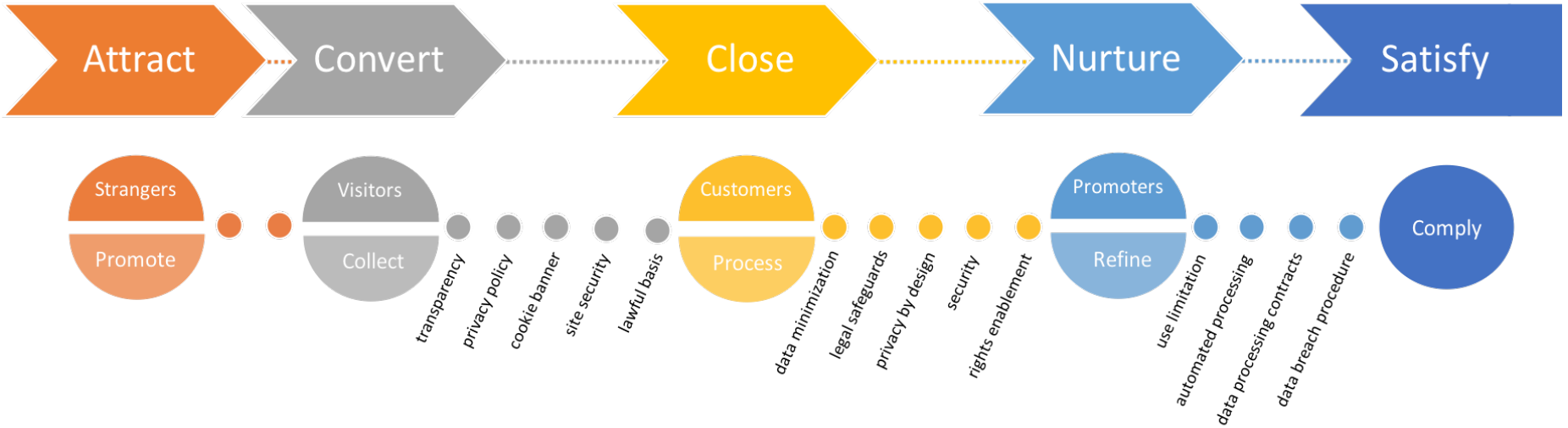
Court of Justice of the European Union

Pre-Ticked Checkboxes on Website Consent Banners are Invalid Forms of Consent

- On 1 October 2019, CJEU decided against Planet49, a German online gaming company for it's website consent practices
  - ✓ 1st - unchecked tick-box to receive third party advertising - to enter the competition, users had to tick this box
  - ✓ 2nd - pre-ticked box allowed Planet49 to use cookies to track user's behaviour online
- Significant effect on the nature of valid consent and how it applies to cookie banners
  - ✓ Pre-ticked boxes are not valid consent
  - ✓ Expiration dates for both the cookies, and any third party sharing of data, should be disclosed to visitors when obtaining consent
  - ✓ Cookies used for different purposes should not be bundled under same consent ask
  - ✓ An active behaviour with a clear view of the consent should be obtained, meaning that, claiming in notices that consent is obtained if users continue to use a website is not an acceptable approach (recently confirmed by Irish DPC's report on cookies)
  - ✓ Rules apply to cookies regardless of whether the data accessed is personal or not
- Basically, if the cookies are not absolutely necessary for the site to operate, they should not be dropped or activated until consent is gained freely, informed specifically and unambiguously

Marketing, Privacy and GDPR

GDPR Impact on Marketing Processes



Strangers / Promote

- Data Acquisition – evidence of lawful gathering for both Purchased/Data Broker Lists and your own in-house lists

Visitors / Collect

- Transparency
- Privacy Policy
- Cookie Banner
- Site Security
- Lawful Basis

Customers / Process

- Data minimization
- Legal Safeguards
- Privacy by Design
- Security
- Rights Enablement

Promoters / Refine

- Use Limitation
- Automated Processing
- Data Processing Contracts
- Data Breach Procedures

Privacy and Data Protection in the Remote Working World

Online Workshop Series "Restart Your Business, Rethink Your Strategy" In Response to COVID-19

GRIFFITH COLLEGE

iSME Irish SME Association

SOVY

Direct Marketing Checklist

Key Considerations (1)

1 Direct marketing governance

- Your business has defined and allocated responsibility for compliance with data protection legislation when carrying out direct marketing activities or roles.
- Your business has approved and published direct marketing policies and procedures, which contain data protection guidance and are routinely reviewed to ensure they remain fit-for-purpose.

2 Direct marketing training

- Your business ensures that you provide data protection training to all staff with direct marketing responsibilities (including temporary staff and contractors).
- You should brief all direct marketing staff on their data protection responsibilities on or shortly after appointment with regular updates to maintain levels of awareness.

3 Lawful basis for direct marketing

- Your business has obtained the necessary consent from individuals for marketing in compliance with data protection legislation
- If you are relying on 'legitimate interests' as the lawful basis for your marketing activities your business has applied the three part test and complies with other marketing laws.

Credits: ICO guidance

Privacy and Data Protection in the Remote Working World

Online Workshop Series
"Restart Your Business, Rethink Your Strategy"
In Response to COVID-19

GRIFFITH COLLEGE

iSME
Irish SME Association

SOVY

Direct Marketing Checklist

Key Considerations (2)

4 Bought-in lists

- Your business has sought assurances about the origins and accuracy of any bought-in marketing lists to ensure that they were compiled fairly and lawfully.
- You should not use bought-in lists for emails, texts or automated calls unless you have proof of 'opt-in' consent within the last six months, which specifically names your business.

5 Marketing lists

- If your business sells marketing lists, all lists were compiled fairly and lawfully and accurately reflect people's wishes.
- You should ask for consent to pass contact details to third parties for marketing, and name those third parties

6 Telephone marketing

- Your business identifies itself when making live marketing calls and only makes them in compliance with data privacy regulations.

7 Electronic mail

- Your business identifies itself when sending electronic marketing messages and ensures you have the initial and ongoing permission of recipients in compliance with current legislation.
- You must ensure that you have prior 'opted-in' consent to send electronic marketing messages by email, text, picture or video messaging.

Credits: ICO guidance

Privacy and Data Protection in the Remote Working World

Online Workshop Series
"Restart Your Business, Rethink Your Strategy"
In Response to COVID-19

GRIFFITH COLLEGE

iSME
Irish SME Association

SOVY

Direct Marketing Checklist

Key Considerations (3)

8 Postal marketing

- Your business only sends marketing mail to named individuals who have not objected to receiving mailings in line with current legislation.
- You should maintain your own 'do not contact' list to screen those who have notified you directly that they object to receiving marketing mailings.

9 Marketing by fax

- Your business identifies itself when sending marketing faxes and sends them only in accordance with the express wishes of recipients in compliance with data protection legislation.
- You should not send marketing faxes to individuals, including sole traders and some partnerships, unless they have specifically consented.

10 Opt-out

- Your business has mechanisms in place to ensure that individuals can opt out of marketing easily.
- It must be as easy to withdraw consent as it was to give it. This means the process of withdrawing consent should be an easily accessible one-step process. If possible, individuals should be able to withdraw their consent using the same method as when they gave it.

11 Retention of personal data

- Your business has a retention policy and procedures in place for the personal data you hold for direct marketing.

Credits: ICO guidance

Privacy and Data Protection in the Remote Working World

Online Workshop Series
"Restart Your Business, Rethink Your Strategy"
In Response to COVID-19

GRIFFITH COLLEGE

iSME
Irish SME Association

SOVY

Privacy

Workplace Conduct

Anti-Fraud

Employee Matters

Trade Rules

Privacy and Data Protection in the Remote Working World

Online Workshop Series "Restart Your Business, Rethink Your Strategy" In Response to COVID-19

GRIFFITH COLLEGE

iSME
Irish SME Association

sovy

Simplifying Business Compliance

for the world's 350 million MSMEs: Micro and Small to Medium-Sized Enterprises

Thank You!

www.sovy.com

GRIFFITH COLLEGE

iSME
Irish SME Association

Online Workshop Series
"Restart Your Business, Rethink Your Strategy"
In Response to COVID-19

sovy