

INTRODUCTION TO DATA PROTECTION

WHAT IS DATA PROTECTION?

Data protection relates to the processing of personal data and the securing and managing of personal data to prevent unauthorised access, misuse, loss or exposure. Organisations must handle data responsibly and in compliance with regulations to protect individuals' rights.

WHY IS DATA PROTECTION IMPORTANT?

- > Ensures compliance with the UK GDPR and Data Protection Act 2018
- > Protects individuals' rights over their personal data
- > Avoids legal penalties and fines (up to £17.5M or 4% of global revenue)
- > Enhances trust between employees, customers, and stakeholders
- > Helps prevent data misuse, fraud, and identity theft

KEY REGULATIONS:



UK GDPR



DATA PROTECTION
ACT 2018



AMENDMENTS FROM
01 JANUARY 2021

WHO NEEDS TO COMPLY?

- ✓ All workers handling personal data on behalf of a company/organisation
- ✓ Employers and organisations processing personal data
- ✓ Third-party vendors handling company data



True or False:

UK GDPR is entirely separate from the EU GDPR.

(answers revealed at the end)

UNDERSTANDING PERSONAL DATA

WHAT IS PERSONAL DATA?

Any information that can identify an individual

Examples: Name, address, phone number, email, license plate, CCTV footage

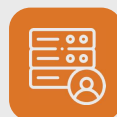


Think about a time you provided personal data (e.g., signing up for an online service). What rights would you have under UK GDPR?

DATA SUBJECT RIGHTS:



Right to be informed
Know how your data is used



Right to access
View the data an organisation holds about you



Right to rectification
Request corrections to incorrect data



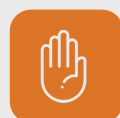
Right to be forgotten
Request deletion of your data



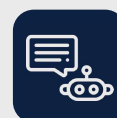
Right to restrict processing
Limit how data is used



Right to data portability
Transfer data between services



Right to object
Request corrections to incorrect data



Rights related to automated decision-making
Ensure human oversight and right to challenge an automated decision that has significant effect

YOUR RESPONSIBILITIES

HANDLING PERSONAL DATA

✓ Stop & Think Before You Share!

✓ Follow Security Best Practices - Use secure systems and passwords

✓ Maintain Confidentiality - Never share without authorisation and be mindful of where you leave personal data if it is in hard copy form

✓ Be Aware of Company Policies - Understand data protection procedures



TRAINING & SUPPORT

- > You Will Be Trained! Tailored to your role.
- > Policies & Governance: Guidelines exist to support you.
- > Single Point of Contact: Your Line Manager can escalate issues to the Data Protection Team.



A colleague asks you to send them a customer's personal data via email. What should you do?

(answers revealed at the end)

- (A) Send it right away.
- (B) Check if it's allowed under the Wincanton policy and ensure security.
- (C) Refuse without checking.

REPORTING DATA INCIDENTS

WHAT IS A DATA BREACH

Accidental, intentional or unlawful destruction, loss, alteration, unauthorised disclosure, or access to personal data

EXAMPLES OF BREACHES:



Phishing emails - providing personal data via suspicious links & requests



Sending personal data to the wrong recipient



CCTV cameras placed in inappropriate locations



Providing access to CCTV footage without authorisation



Providing a delivery note to the wrong customer



Making a delivery to a neighbour and providing them with the paperwork for the delivery rather than posting it through the letterbox of the intended recipient

HOW TO REPORT A BREACH:

01

CONTACT

Contact your Wincanton supervisor [or other relevant point of contact] and notify them of the breach

02

REPORT

Report potential breaches IMMEDIATELY! We have a legal obligation to notify relevant breaches to the ICO within a very short deadline. Delay in reporting could result in us breaching this requirement.



You finish your shift and as you are leaving notice there is a packing slip on the floor containing a customer's name and address. What do you do?

(answers revealed at the end)

- (A) Ignore it
- (B) Pick it up and hand it to your Wincanton supervisor
- (C) Pick it up and put it in the bin

CCTV & FINAL REMINDERS

CCTV USAGE IN WINCANTONS OPERATIONS:

- ✓ Must comply with Wincanton's Surveillance Technologies Policy
- ✓ Cameras must be appropriately sited
- ✓ Access restricted to authorised staff
- ✓ Signage must inform individuals of CCTV in operation
- ✓ Footage must be secure & only accessed for approved reasons
- ✓ Any requests for access to footage should be reported to your Wincanton contact

FINAL REMINDERS:



Always handle data responsibly



If unsure, ask your Wincanton supervisor or contact the Wincanton Data Protection Team



Questions? Email the Data Protection Team at dpo@wincanton.co.uk



In this scenario, you are a delivery driver, delivering parcels to customers home. You're involved in a minor Road Traffic Incident, and one of the other parties involved requests a copy of your dashcam footage. What do you do?

(answers revealed at the end)

- (A) Provide the footage immediately
- (B) Check policy and confirm if access is authorised
- (C) Refuse outright

THE ANSWERS

Please see below for the answers from the questions on each of the pages
- how many did you get right?



Page 1 - False

The UK GDPR is based on the EU GDPR and was enacted to ensure continuity after Brexit



Page 3 - B

Always verify the legitimacy of requests before sharing! If you are not sure, always check - this can avoid a data breach



Page 4 - B

Always report any instances where personal data is somewhere other than where it is supposed to be. Personal data needs to be securely destroyed, so it is not appropriate to put it in the general purpose bin.



Page 5 - B

Always follow Wincanton policy when handling sensitive data!