

Data Privacy Fundamentals



- Data privacy means handling personal info responsibly, not just following legal rules



- It protects people, builds trust, and shields the company from real harm



- Agenda: key concepts, daily habits, and practical scenarios you can use immediately



Privacy vs. Security: Two Sides of the Same Coin

- ✓ Privacy is about "should we": rules for responsible data use and consent
- ✓ Security is about "can we": safeguards blocking unauthorized access
- ✓ Strong security can exist without privacy, but not true privacy without security
- ✓ Privacy governs collection and use; security protects with technical controls



Privacy

Focused on people and data rights. Ensures information is collected, used, and shared responsibly.



Security

Focused on systems and protection. Prevents unauthorized access, breaches, and data loss.



Privacy sets the rules for ethical data use.



Security provides the safeguards that make those rules possible.



Why This Matters: Real-World Consequences



Reputational damage: lost trust from customers, partners, and employees



Operational disruption: incident response, system lockdowns, and remediation



Regulatory fallout: GDPR fines up to 4% of global turnover, mandatory breach notifications



Personal Data: Recognizing It Every Day



Personal data is any information that can identify a person directly or indirectly



Common workplace examples: name, email, phone, employee ID, IP address, job title



Even seemingly small pieces of data can combine to identify someone when linked together



Payroll registers, address lists, and sick leave records are also personal data



HR systems are concentrated repositories of this data, requiring careful handling



The Data Ripple

Every piece of data creates a ripple. Together, they can reveal who someone is.

Sensitive Data:

When Extra Care Is Required



- Sensitive data demands heightened protection by law (GDPR Article 9)



- Examples: health records, biometrics, ethnic origin, trade union membership



- Financial account details and bank information require elevated safeguards



- In HR: sick leave documentation, disability accommodations, background check results



The Core Principles: Collect, Use, and Keep Only What You Need



Data minimization:

collect only what is adequate, relevant, and necessary



Purpose limitation:

use data only for the specific reason it was collected



Storage limitation:

retain personal data only as long as required, then delete or anonymize

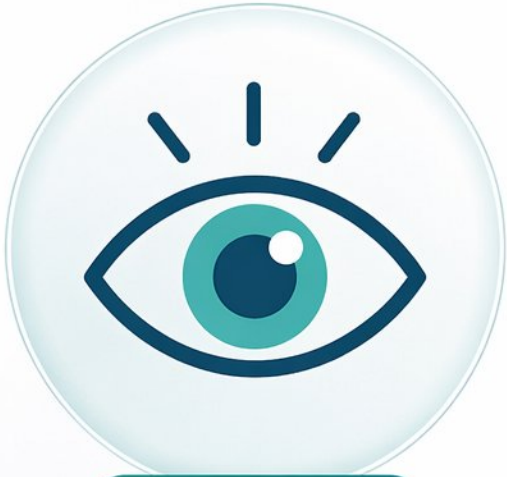


Apply to everything:

emails, forms, shared drives, and HR records



People Have Rights: Access, Correction, and Deletion



Access



Correction



Deletion

- Individuals can request a copy of all personal data you hold about them
- They can demand correction of inaccurate or incomplete information immediately
- They can request deletion when there's no longer a legal basis to keep it
- HR must respond to these requests within one month under GDPR
- Legal retention obligations may override deletion requests for certain records





Privacy in Daily Workflows: Email and Messaging

- - Verify recipients before sending: autocomplete is a top misdirection risk
- - Use BCC for mass mail; avoid needless reply-all chains
- - Share sensitive data via secure links with view-only permissions
- - Never treat “please delete” as a reliable remediation



Privacy in Daily Workflows: Shared Drives and Collaboration Tools



- Set permissions to Viewer or Commenter, not Editor by default



- Regularly audit and remove stale shared links and external access



- Never store sensitive business data in personal drives or accounts



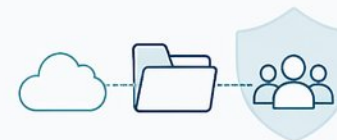
- Use Shared Drives—not My Drive—for team-owned business files



- Before sending, confirm link scope, permission level, and recipients



Principle: Grant the least access necessary.
Review regularly. Protect always.



Privacy in Daily Workflows: Physical Spaces and Devices



- Lock away sensitive documents and portable media when not in use



- Lock your screen every time you step away



- Shred paper documents containing personal data; never toss in recycling



- Use privacy screens in public spaces and never leave devices unattended



Phishing and Social Engineering: Spot the Red Flags



- **Urgency and pressure:** "Act now or your account will be suspended"



- **Impersonation:** fake executives, IT support, recruiters, or vendors



- **Unexpected attachments or links** from altered or unknown domains



- **Fake job interview scams** impersonating major brands to steal credentials



- **Vishing calls** posing as IT to capture MFA codes or enroll their own passkeys



Phishing in 2026: Modern Tactics Targeting the Workplace



01

Fake job interviews impersonating Netflix, Adobe, and Coca-Cola to steal credentials



02

IT support vishing calls that trick you into enrolling an attacker's passkey



03

Hijacked vendor email threads used to redirect payments to fraudulent accounts



04

Fake Microsoft passkey setup ceremonies that distract you during account takeover



05

Nested redirects through legitimate services to hide malicious landing pages



I Spot a Red Flag—What Do I Do?



When something feels off, **trust your instincts.**



Don't Interact

- Don't click, don't reply, don't forward the suspicious message



Report It

- Report it immediately through the company's designated reporting channel



Notify IT or Security

- If you accidentally engaged, notify IT or security right away



Never share MFA codes or approve unexpected prompts on a call





Working Remotely: Securing Your Connection



- Always use a company VPN on any network outside the office



- Never rely on public Wi-Fi without a VPN—attackers can intercept traffic or set up fake "evil twin" hotspots



- Use a personal mobile hotspot as a safer alternative when VPN is unavailable



SECURE CONNECTION

With Company VPN



VS.



PUBLIC WI-FI CONNECTION

Without VPN



Encrypted. Private. Protected.
Your data is secure.



Unencrypted. Exposed. At Risk.
Attackers can intercept or steal your data.

Working Remotely: Device and Data Hygiene



- Keep work and personal accounts completely separate; never forward work emails to personal inboxes



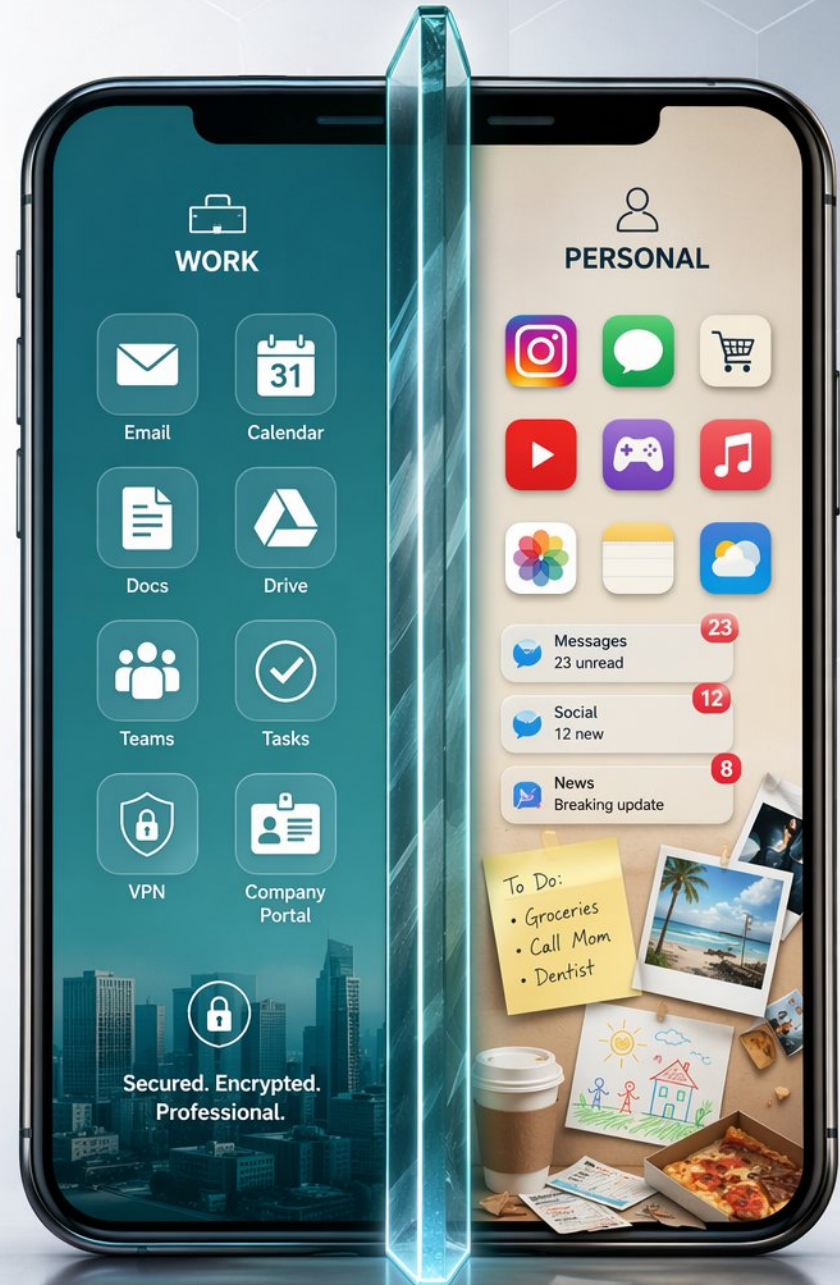
- Enable screen locks, automatic OS updates, and full-disk encryption on all devices



- Use privacy screens in public spaces and never leave devices or documents unattended



- Avoid discussing confidential information within earshot of strangers in public places



BOUNDARY PROTECTS
DATA AND TRUST

Bring Your Own Device (BYOD): Know the Rules



- Only access company data if explicitly permitted by policy



- Approved devices need MDM, endpoint protection, and encryption



- Report lost or stolen devices immediately for remote wipe



- Never store work data in personal accounts or unapproved apps

MANDATORY SECURITY CONTROLS



MDM



Endpoint Protection



Encrypted Storage



If Something Goes Wrong: Reporting Steps

1

Accidents happen: lost device, misdirected email, unauthorized access—don't panic

2

Notify your manager and privacy/security team immediately

3

Provide details: what happened, when, and what data was involved

4

Early reporting protects everyone and meets legal deadlines (often 72 hours)



What Not to Do After an Incident



Do not delete evidence, hide the mistake, or try to fix it on your own



Do not forward the exposed data to yourself or anyone else as a 'backup'



Do not contact external recipients directly unless instructed



Report immediately: what happened, when, and what data was involved



The security team will handle containment and determine next steps



Building Your Privacy Habit: Practical Micro-Commitments

1

- Pause before sending: check recipients and attachments on sensitive emails

2

- Challenge unnecessary data requests: "Do you really need this?"

3

- Lock your screen and secure your workspace every time you step away

4

- Default to Viewer or Commenter—not Editor—when sharing files

5

- Connect to the VPN before opening any internal apps or files



Quick Recap and Your Privacy Toolkit



- 1 Privacy is about 'should we'; security is about 'can we'



- 2 Personal data identifies you; sensitive data demands extra protection



- 3 Collect only what you need, use it only for the stated purpose, delete it when done



- 4 Pause before sending, challenge unnecessary data requests, secure your workspace



- 5 Spot urgency, impersonation, and unexpected attachments; report, don't click



- 6 Always use a VPN on public Wi-Fi; report incidents immediately, don't hide mistakes



PersonWise.

PersonWise • AI digital-human course platform



Scan the code or click anywhere to watch this course live, with voice Q&A

personwise.ai/t/ec02d523/public