Fellowes

Bedrijfs-checklist

Ondersteuning van **AVG**-naleving en afstemming op **NIS-2**-regelgeving

Samen sterk in compliance

1 Houd beleid actueel

- Herzie "Bring-Your-Own-Device"-regels en neem richtlijnen op voor thuiswerken.
- Behandel de risico's van openbaar / thuis-Wi-Fi en hoe medewerkers veilig verbinding maken..
- Werk beleid bij over het printen, opslaan en vernietigen van papieren documenten (zowel op kantoor als thuis).
- Versterk wachtwoordrichtlijnen (bijv. drie-woord-wachtzinnen, MFA).
- Vereis veilige gegevenswissing voordat IT-apparatuur wordt weggegooid.

2 Bied regelmatige training

- Leid medewerkers op in AVG-basisprincipes, gegevensverwerking en de zes kernprincipes van gegevensbescherming.
- Neem ook verwerking van gevoelige papieren documenten en bewaartermijnen mee.
- Voeg modules toe over thuiswerkbeveiliging en nieuw beleid.
- Gebruik een online trainingsportaal om voortgang en deadlines bij te houden.
- Bied praktische hulpmiddelen zoals een checklist of zelfevaluatie ("Data Security Health Check").
- Verwijs naar NIS2 in trainingen als extra laag van cyberweerbaarheid, vooral voor IT- en securityteams.

3 Voorzie medewerkers van de juiste middelen

- Voorzie werknemers van bedrijfslaptops in plaats van afhankelijk te zijn van persoonlijke apparaten (BYOD).
- Investeer in sterke antivirus- en firewalloplossingen.
- Zorg voor toegang tot papierversnipperaars: kantoormodellen op de werkplek en compacte shredders voor thuis.
- Gebruik micro-cut (P-5) shredders voor zeer vertrouwelijke gegevens.
- Geef prioriteit aan productiviteit en veiligheidsfuncties (bijv. papierstoring voorkomen, veilig gebruik).

4 Communiceer consequent

- Benadruk beveiliging op alle niveaus; verklein kennisgaten bij junior medewerkers.
- Bespreek dataveiligheid in locatievergaderingen, teamoverleggen en 1-op-1's.
- Deel beleidsupdates via posters, nieuwsbrieven en intranet.
- Verspreid phishing-/cyberaanvalwaarschuwingen en best practices binnen het bedrijf.
- Maak gegevensbescherming een vast agendapunt in kwartaalbesprekingen.
- Positioneer AVG als basis van compliance, met NIS2 als versterking van de cybersecuritycultuur.

Fellowes

Medewerkers-checklist

Ondersteuning van **AVG**-naleving en afstemming op **NIS-2**-regelgeving

Blijf veilig omgaan met gegevens

1 Bescherm uw digitale gegevens

- Gebruik sterke, unieke wachtwoorden en sla ze op in een wachtwoordmanager. ☐
- Schakel tweefactorauthenticatie in. ☐
- Wees alert op phishing – klik niet op verdachte links of bijlagen. ☐
- Houd apparaten versleuteld, up-to-date, beveiligd met wachtwoord en voorzien van antivirus. ☐
- Gebruik altijd de bedrijfs-VPN bij werken op afstand; vermijd openbaar Wi-Fi tenzij toegestaan. ☐
- Volg bedrijfsregels bij gebruik van persoonlijke apparaten (BYOD). ☐

2 Ga correct om met gevoelige papieren gegevens

- Weet wat als gevoelig telt: persoonsgegevens, bedrijfsadministratie, HR-dossiers, financiële documenten. ☐
- Versnipper documenten zodra bewaartermijnen zijn verstreken (bijv. contracten, HR-dossiers, bonnen, afschriften). ☐
- Laat geen papieren documenten slingeren – ruim dagelijks je bureau op en berg documenten veilig op. ☐
- Denk na voordat je print – alleen als het echt nodig is. ☐
- Versnipper gevoelige documenten altijd vóór weggooien, nooit direct in de papierbak. ☐
- Evalueer opgeslagen documenten regelmatig en anonimiseer persoonsgegevens waar mogelijk. ☐

3 Blijf compliant met beleid en training

- Volg verplichte trainingen en opfriscursussen regelmatig. ☐
- Spreek collega's aan als je risicovol gedrag ziet. ☐
- Ken de zes kernprincipes van gegevensbescherming. ☐
- Raadpleeg je manager of Data Protection Officer bij twijfel over beleid of omgang met data ☐
- Blijf op de hoogte van wijzigingen in bedrijfsbeleid of privacywetgeving (zoals NIS-2). ☐