

Bijlage 6. Email, internet en sociale media

We begeven ons steeds meer in een digitaal tijdperk. Alle werknemers komen in aanraking met internet, e-mail en sociale media. Daarom is het belangrijk goede richtlijnen te voorzien over het gebruik van deze technologieën.

In dat verband wordt verwezen naar de door de werkgever uitgevaardigde policies en richtlijnen m.b.t. email internet en sociale media gebruik. In deze bijlage worden enkel de belangrijkste verplichtingen en de controlemodaliteiten voor email en internet bepaald.

Het reglement is opgesteld overeenkomstig de bepalingen van de collectieve arbeidsovereenkomst nr. 81 en de Algemene Verordening Gegevensbescherming.

1) Toepassingsgebied

Deze policy is van toepassing op alle werknemers van Renewi met betrekking tot:

- door Renewi ter beschikking gestelde e-mailadressen;
- door Renewi verschaft toegang tot internet; en
- het gebruik van sociale media.

2) Gebruik van e-mail

De door Renewi ter beschikking gestelde e-mailadres en systeem is primair bestemd voor professioneel gebruik. De werknemer mag zijn professioneel e-mailadres echter beperkt gebruiken voor persoonlijke doeleinden. Deze e-mails dient de werknemers dan als "privé" te classificeren. Omgekeerd mag een privé email adres nooit gebruikt worden voor zakelijke doeleinden.

De toegang tot of het gebruik van het e-mailadres mag nooit doorgeven worden aan derden.

Het is strikt verboden om de e-mail te gebruiken voor:

- het verspreiden van vertrouwelijke gegevens over de onderneming (behalve indien vereist in het kader van het werk);
- het verspreiden van gegevens die de auteursrechten schenden;
- het verspreiden of het doorsturen van berichten die de een inbreuk vormen op de waardigheid van anderen;
- het versturen of doorsturen van berichten die ingaan tegen de openbare orde en de goede zeden;
- deelname aan kettingsmails;
- het uitoefenen van een beroepsactiviteit buiten de onderneming;
- het verrichten van illegale activiteiten of handelingen.

Werknemers moeten de vertrouwelijkheid van andermans elektronische communicaties respecteren en mogen zich niet ter kwader trouw toegang verschaffen tot de elektronische berichten van andere werknemers of derden, noch mogen zij deze lezen zonder voorafgaande toestemming.

Werknemers dienen alle veiligheidsregels inzake ICT na te leven en de instructies van de IT diensten terzake op te volgen.

3) Gebruik van Internet

De toegang tot internet is bestemd voor professioneel gebruik.

Het gebruik voor privé-doeleinden wordt geduld binnen de volgende beperkingen:

- uitsluitend tijdens de pauzes;
- enkel raadpleging van algemene websites (zoals online kranten, weersites, openbaar vervoer, verkeersinformatie) met een geoorloofde inhoud.

Het is ten strengste verboden om internet te gebruiken (professioneel of privé-gebruik) voor:

- het raadplegen van websites met ongeoorloofde content;
- het raadplegen van online spelletjessites;
- het raadplegen van websites waarvan de toegang betalend is en waarvoor registratie vereist is (met uitzondering van de professionele websites waarop de werkgever ingeschreven is);
- het raadplegen van en deelnemen aan discussieforums, blogs (met uitzondering van de professionele forums waaraan de werkgever wenst deel te nemen);
- het illegaal downloaden van auteursrechtelijk beschermde gegevens;
- het meedelen van het professioneel e-mailadres op de bezochte websites;



- het downloaden van programma's, muziek of andere (met uitzondering van de professionele websites waarop de werkgever is ingeschreven en die deze downloads toelaten).

Deze lijst is niet beperkend.

4) Gebruik van sociale media

De toegang tot en het gebruik van sociale media op de werkvloer behoort steeds tot de exclusieve beslissingsbevoegdheid van de werkgever.

De onderneming verkiest echter om Sociale Media te benutten op diverse vlakken. Zo kunnen sociale media aangewend worden om een merk te versterken, maar ook om in contact te komen met potentiële klanten en potentiële werknemers.

Verder kan er kennis en informatie over de ondernemingsactiviteit gedeeld worden met de werknemers, leveranciers en klanten. Sociale media zorgen in toenemende mate voor het imago van de onderneming.

De onderneming verkiest bovendien om als één merknaam naar buiten te treden waardoor deelaccounts niet toegestaan zijn.

Volgende basisregels dienen te worden gerespecteerd :

- Volg altijd de algemene gedragsregels van het bedrijf. Deze gelden ook voor sociale media.
- Respecteer auteursrechten, gebruik geen materiaal van anderen zonder toestemming. Maak eventuele bronnen kenbaar;
- Spreek niet slecht over partners en concurrenten noch over het bedrijf;
- Verspreid nooit interne (bedrijfs)informatie;
- Gebruik nooit de bedrijfsnaam of het bedrijfslogo in je profielnaam en -foto;
- Maak zeker geen profielen aan onder de bedrijfsnaam ook niet voor welbepaalde projecten;
- Treed niet op als woordvoerder van je werkgever;
- Citeer geen collega's en gebruik niet zijn of haar materiaal zonder toestemming;
- Plaats geen verdeckte marketingboodschappen of spam;
- Reageer nooit op juridische kwesties of crisissituaties (zoals ongevallen of brand), maar licht je leidinggevende in;
- Verspreid geen berichten die de een inbreuk vormen op de waardigheid van anderen.

5) Controlemodaliteiten email en internet

a) Doeleinden van de controle (finaliteit)

De werkgever heeft het recht om te controleren welk gebruik zijn werknemers maken van de hulpmiddelen die hen ter beschikking worden gesteld.

De werkgever gaat over tot de controle van het gebruik van e-mail en Internet met het oog op:

- Het voorkomen van illegale of lasterlijke feiten, feiten die strijdig zijn met de goede zeden of de waardigheid van andere personen kunnen schaden;

Het betreft onder andere: het kraken van computers, het raadplegen van pornografische of pedofiele sites of sites die aanzetten tot discriminatie, rassenscheiding, haat of geweld jegens een groep, een gemeenschap of de leden ervan, wegens ras, huidskleur, afkomst, religie of nationale of etnische afstamming van deze leden of van sommigen onder hen.

- Het beschermen van de economische, commerciële en financiële belangen van de onderneming die vertrouwelijk van aard zijn, alsook het tegengaan van ermee in strijd zijnde praktijken;

Het betreft onder meer bepaalde daden van afbrekende publiciteit, het verspreiden van bestanden en de schending van zakengeheimen, met inbegrip van onderzoek en ontwikkeling, productieprocessen en alle mogelijke vertrouwelijke gegevens.

- Het verzekeren of herstellen van de veiligheid en/of de goede technische werking van de IT-netwerksystemen van de onderneming, met inbegrip van de controle op de kosten die ermee gepaard gaan, alsook de fysieke bescherming van de installaties van de onderneming;

Het gaat er meer bepaald om overbelasting van het netwerk of verspreiding van virussen te vermijden of op te lossen.

- Ervoor te zorgen dat de in de onderneming geldende beginselen en regels voor gebruik van de onlinetechnologieën te goeder trouw nageleefd worden.

b) Proportionaliteit

In principe mag de controle op de elektronische online communicatiegegevens geen inmenging in de persoonlijke levenssfeer van de werknemer tot gevolg hebben. Als de controle toch een inmenging in de persoonlijke levenssfeer van de werknemer tot gevolg heeft, moet deze inmenging tot een minimum beperkt worden.

c) Globale controle

De controle kan op elk ogenblik globaal gebeuren. Het globale karakter van de controle houdt in dat de controle bestaat uit:

- het verzamelen van het aantal e-mails die werden ontvangen of verstuurd per werkpost, het bijhouden van het volume van de mails en van het formaat van de bijlagen;
- het bijhouden van de bezochte websites en van het moment waarop de aansluiting gebeurde en de duur van de aansluiting.

6) Opvolging van de controle email en internet gebruik: procedure bij vaststelling van onregelmatigheid

a) Directe en indirecte individualisering

Wanneer, als gevolg van een globale controle, de werkgever een onregelmatigheid vaststelt, gaat hij over tot een individualisering van de gegevens om de werknemer die verantwoordelijk is voor deze onregelmatigheid te identificeren.

- Deze **individualisering is direct** wanneer het doel van de globale controle bestaat uit:
 - het voorkomen van ongeoorloofde of lasterlijke feiten, feiten die strijdig zijn met de goede zeden of de waardigheid van andere personen kunnen schaden;
 - het beschermen van de economische, commerciële en financiële belangen van de onderneming die vertrouwelijk van aard zijn, alsook het tegengaan van ermee in strijd zijnde praktijken;
 - het verzekeren of herstellen van de veiligheid en/of de goede technische werking van de IT-netwerksystemen van de onderneming, met inbegrip van de controle op de kosten die ermee gepaard gaan, alsook de fysieke bescherming van de installaties van de onderneming.

Directe individualisering betekent dat de werkgever overgaat tot het identificeren van de werknemer die verantwoordelijk is voor de onregelmatigheid zonder enige voorafgaande verwittiging.

- De **individualisering is indirect** wanneer het doel van de globale controle erin bestaat na te gaan of de werknemers de bepalingen van dit reglement naleven.

In dat geval waarschuwt de werkgever de werknemers ervan dat er onregelmatigheden werden vastgesteld tijdens een globale controle en dat de gegevens geïndividualiseerd zullen worden indien in de toekomst opnieuw dergelijke onregelmatigheden worden vastgesteld.

Wanneer de werkgever een werknemer die de onregelmatigheid heeft begaan, wenst te sanctioneren, nodigt hij hem uit voor een voorafgaand gesprek zodat de werknemer uitleg kan geven over zijn gebruik van e-mail en Internet.

Dit gesprek wordt niet georganiseerd wanneer de arbeidsovereenkomst van de werknemer, bij de vaststelling van de feiten, om gelijk welke reden is geschorst.

b) Rechten en plichten van de personen die instaan voor de controle

De personen bevoegd voor het uitvoeren van de controle is de HR director in samenwerking met de ICT verantwoordelijke.

Zij zijn bevoegd om:

- de globale controle te laten uitvoeren door de ICT verantwoordelijke;
- te oordelen of er moet worden overgegaan tot directe en indirecte individualisering;
- de werknemers te informeren over de stappen die ze moeten ondernemen wanneer ze verdachte e-mails ontvangen of kennis nemen van verdachte zaken op geraadpleegde websites;
- het voorafgaand gesprek te voeren met de werknemer n.a.v. een controle. De betrokken medewerker kan zich laten bijstaan door een vertegenwoordiger van de syndicale delegatie.

c) Bewaren van persoonlijke gegevens

De persoonlijke gegevens die worden verzameld tijdens een controle worden bewaard gedurende een periode van 12 maanden op de ICT afdeling.

De werknemer heeft het recht om kennis te nemen van zijn persoonlijke gegevens die werden verzameld tijdens de controle en om de werkgever te verzoeken eventueel foute gegevens te wijzigen of te schrappen.

7) Sancties

Aan de werknemer die de bepalingen van het reglement niet naleeft, kan één van de sancties worden opgelegd vermeld in het arbeidsreglement.

Wanneer de werknemer dit reglement herhaaldelijk overtreedt, wanneer het een ernstige overtreding betreft of wanneer zijn handelwijze schade berokkent aan de werkgever, kan hij worden ontslagen om dringende redenen zonder opzegging noch vergoeding.