Privacy op de werkplek

De Wet betreffende de arbeidsovereenkomsten verplicht de werknemer te handelen volgens de bevelen en instructies die hem worden gegeven door de werkgever met het oog op de uitvoering van de arbeidsovereenkomst. Dit is een voldoende basis om tussenkomsten en beperkingen te rechtvaardigen die voortvloeien uit de normale uitoefening van het gezag door de werkgever. Maar de werkgever mag zijn macht niet misbruiken ten nadele van het recht op privacy van de werknemer.

Sinds 25 mei 2018 vult de Algemene Verordening Gegevensbescherming (AVG) de al bestaande bepalingen aan die de arbeidsrelatie regelen. De AVG bepaalt strikter de verplichtingen van de werkgever.

De arbeidsverhoudingen tussen werknemer en werkgever vormen echter een specifiek domein voor de bescherming van de persoonsgegevens. Er is sprake van twee conflicterende principes:

> enerzijds het gezag van de werkgever over zijn werknemer en de daaruit voortvloeiende ondergeschiktheid. Een werkgever kan dus instructies geven aan zijn werknemers en hun prestaties controleren;
> anderzijds het recht op privacy van de werknemers, waardoor het voor de werkgever verboden is zijn gezag uit te oefenen over de persoonlijke aspecten en activiteiten van zijn werknemers.

Hoewel de AVG tot doel heeft de regels over de bescherming van persoonsgegevens binnen de Europese Unie te harmoniseren, voorziet ze in een uitzondering op het gebied van de arbeidsrelaties, net door de karakteristieke relatie tussen werkgever en werknemer. Het is zodoende mogelijk specifieke regels op te stellen voor de verwerking van persoonsgegevens van werknemers, zowel op sector- als op bedrijfsniveau, bv. via collectieve arbeidsovereenkomsten.

Gegevens van de werknemers

De werknemer behoudt (een deel van) zijn privacy op de werkvloer. Dit betekent echter niet dat de werkgever geen persoonsgegevens van zijn werknemers zou mogen verwerken of dat hij geen (elektronisch) toezicht mag uitoefenen op diezelfde werknemer. Het feit dat iemand een arbeidsovereenkomst sluit, impliceert dat deze persoon als werknemer instemt met een aantal beperkingen op de uitoefening van zijn grondrecht op privacy.

Een aantal van de veel voorkomende verwerkingen van persoonsgegevens van werknemers kunnen hieronder reeds geraadpleegd worden.

Toezicht van de Werkgever

Toezicht op de werkvloer gebeurt meer en meer op een elektronische manier. Aangezien e-mail, internet en andere ICT-toepassingen (zoals geolokalisatie en camerabewaking) hun weg gevonden hebben naar de werkvloer, stellen zowel werkgevers als werknemers steeds meer vragen over deze "moderne" vorm van gezagsuitoefening.

Terecht, in tegenstelling tot vroeger (waarbij de gezagsuitoefening eerder visueel en face to face gebeurde) bieden de controle-instrumenten waarover een werkgever vandaag beschikt technische mogelijkheden die bijzonder indringend kunnen zijn en dus een gevaar kunnen opleveren voor de privacy van de gecontroleerde werknemer.

Net daarom dat de Autoriteit aan een aantal van deze elektronische toepassingen bijkomende aandacht schenkt.

Gevoelige gegevens

De Algemene Verordening Gegevensbescherming (AVG) verbiedt in beginsel de verwerking van gevoelige gegevens op de werkvloer. Niettemin kan de werkgever in een aantal gevallen toch deze gegevens opvragen en gebruiken.

Sociale netwerken op de werkplek

In de hedendaagse maatschappij communiceren we steeds meer via sociale netwerken (Facebook, Twitter, Netlog, LinkedIn, ...). Ondernemingen doen dat ook. Ze maken massaal gebruik van sociale netwerken voor zakelijke doeleinden. Daarom hebben werknemers ook steeds vaker toegang tot sociale netwerken binnen het bedrijf om hun taken te kunnen uitvoeren.

Dat de grens tussen beroepsactiviteiten en privésfeer in dat verband dus niet altijd even duidelijk is, hoeft niet te verbazen.

Hoe zit het nu echt? Kan een werkgever controleren of een werknemer tijdens de werkuren op sociale netwerken actief is? Kan een werknemer zich op Facebook afreageren op zijn werkgever? Kan een werknemer ontslagen worden omdat hij compromitterende zaken over zijn bedrijf op een sociaal netwerk heeft gepost? Mag een werkgever op Facebook controleren of een werknemer op een bepaalde dag echt ziek was? Mag een werkgever in het geheim de Facebook-pagina van een werknemer lezen, zelfs als de werknemer er alleen in zijn vrije tijd op actief is?

Helaas is het antwoord niet altijd even eenvoudig of eenduidig. Het hangt vaak af van een combinatie van omstandigheden waarbij de moeilijkheid ligt in het vermogen een duidelijke grens te trekken tussen het privé- en beroepsleven enerzijds en het belang van de werkgever en dat van de werknemer bij het respecteren van de privacy anderzijds. Het is niet ongebruikelijk dat dergelijke geschillen uiteindelijk voor de rechter komen.

Er bestaat momenteel geen specifieke wetgeving over het gebruik van sociale netwerken op de werkplek.

Zeker is wel dat:

- het recht op privacy een fundamenteel recht is dat voor iedereen geldt en iedereen heeft recht op bescherming van zijn persoonsgegevens. In België wordt het recht op bescherming van de persoonsgegevens verplicht gesteld door de AVG;
- de werkgever bepaalt of en voor welke doeleinden hij zijn werknemers toegang verschaft tot sociale netwerken; hij kan besluiten dat sociale netwerken op de werkplek voor privédoeleinden mogen worden gebruikt en op welke tijden van de dag dit is toegestaan;
- de werkgever heeft een controlerecht dat weliswaar niet onbeperkt is, maar hij kan wel controleren of de werknemer zich aan diens voorschriften houdt;
- de werkgever moet de controle op het gebruik van sociale netwerken op de werkplek via het arbeidsreglement melden. Het moet de werknemer dus duidelijk zijn wanneer en waarom de werkgever een controle uitvoert;
- het onderscheid tussen een privébericht en een professionele boodschap op een sociaal netwerk is niet altijd duidelijk. Soms moet de rechtbank hierover beslissen;
- de werkgever mag het gebruik van sociale netwerken buiten de werkuren niet verbieden; hij mag evenmin de activiteiten van de werknemer op sociale netwerken tijdens zijn vrije tijd en verlofdagen controleren;
- de werknemer mag geen lasterlijke commentaren op een sociaal netwerk posten over zijn werkgever, noch belangrijke of gevoelige professionele informatie onthullen, ook niet buiten de werkuren. Dit kan leiden tot een onmiddellijk ontslag. Hier bestaat jurisprudentie over.

In ieder geval moeten de werknemers zich ervan bewust zijn dat de werkgever hoort en ziet wat er om hen heen gebeurt. Het is daarom belangrijk informatie niet ondoordacht te delen op een sociaal netwerk.

De eID op de werkplek

Elke Belg heeft een (elektronische) identiteitskaart. Vroeger werd de identiteitskaart uitsluitend gebruikt voor administratieve verplichtingen tegenover de gemeente en de politie, maar met de elektronische identiteitskaart (de eID) is het ook mogelijk officiële documenten te ondertekenen en controles uit te voeren.

De eID is een elektronisch identiteitsbewijs dat kan worden gebruikt voor identificatie- en authenticatiedoeleinden. De kaart bevat gevoelige gegevens die zowel op de kaart worden afgedrukt als op de chip worden opgeslagen in een elektronisch bestand. De gegevens omvatten o.a. de naam, voornamen, nationaliteit, geboortedatum en -plaats, geslacht, foto en rijksregisternummer. Ondertussen bevat de identiteitskaart ook de digitale vingerafdrukken van de kaarthouder. De GBA heeft zich meerdere malen uitgesproken over dit onderwerp.

Onze identiteitskaart bevat persoonsgegevens die beschermd moeten worden.

Verzoek om eID voor te leggen

Een werkgever kan de eID van een (kandidaat-)werknemer vragen als hij daar een goede reden voor heeft. Tijdens het aanwervingsproces zal dat bv. gebeuren:

> wanneer de werkgever kandidaat-werknemers uitnodigt op basis van de resultaten van een toelatingstest. In dit geval kan de werkgever de kandidaat-werknemer vragen zijn identiteit te bewijzen zodat er geen twijfel kan bestaan over de resultaten die hij heeft behaald.
> de situatie waarin de werkgever moet controleren of de werknemer over bepaalde kwalificaties of werkvergunningen beschikt. Hij moet dan de identiteit van de kandidaat-werknemer kennen en deze kunnen vergelijken met de identiteit die op de desbetreffende kwalificaties of werkvergunningen wordt vermeld.

Ook uitzendbureaus kunnen de eID van werkzoekenden vragen. Net als elke andere werkgever moet een uitzendbureau na het sluiten van een arbeidsovereenkomst voldoen aan allerlei socialezekerheidsverplichtingen. In het geval van uitzendwerk zit er vaak heel weinig tijd tussen de selectie van een kandidaat voor een uitzendbaan en zijn indiensttreding. Het uitzendbureau kan de eID (inclusief het rijksregisternummer) van de uitzendkracht dus opvragen en uitlezen zodra deze is ingeschreven, met het oog op zijn indiensttreding.

Inloggen en ondertekenen van documenten via de eID

De eID is ontworpen om burgers betrouwbaar te authenticeren en documenten in digitale vorm te ondertekenen.

Het is dan ook begrijpelijk dat werkgevers deze mogelijkheid willen gebruiken. De chip in de eID heeft twee aparte sleutels waarmee de houder van de kaart:

> zijn identiteit aan derden kan bewijzen (authenticatiesleutel);
> zijn identiteit kan bewijzen en de inhoud van een document kan ondertekenen (sleutel voor digitale handtekeningen).

Om beide certificaten te kunnen gebruiken, moet de eID-houder zijn pincode invoeren.

Merk op dat elke sleutel wordt geleverd met een certificaat. Dit certificaat is een bestand met onder andere de naam, de voornamen en het rijksregisternummer van de betrokkene, samen met een aantal technische gegevens gerelateerd aan de sleutel.

De werkgever kan de eID gebruiken om werknemers toegang te verschaffen tot de computersystemen van het bedrijf. De werkgever moet echter een goede reden hebben om de eID te gebruiken als identificatiesleutel voor de informaticasystemen van het bedrijf. Bovendien moet hij de werknemer altijd vooraf informeren over het gebruik van de eID door de werkgever.

De instructie documenten met behulp van de eID te ondertekenen kan alleen worden gegeven voor documenten die binnen het kader van de taken van de betrokken werknemer vallen en enkel als een eenvoudige handtekening niet volstaat.

Vermits de werkgever de verwerkingsverantwoordelijke is voor de persoonsgegevens die worden verwerkt wanneer een elektronische handtekening met behulp van de eID wordt aangebracht, moet hij passende technische en organisatorische maatregelen treffen om de persoonsgegevens te beschermen van zijn werknemers die hun eID gebruiken om professionele documenten te ondertekenen. Dit betekent concreet dat de werkgever voldoende middelen moet inzetten om zijn computersystemen te beschermen tegen kwaadaardige software (malware) die bedoeld is om mensen te verleiden tot het ondertekenen van documenten zonder hun medeweten of waarvan de inhoud niet is wat ze denken.

De regeling van waarschuwingssystemen conform de privacyregels

Een waarschuwingssysteem verwijst naar het geheel van interne procedures waarmee het bestaan van een specifiek misbruik binnen het bedrijf of de overheid kan worden gemeld (wie kan wat melden, aan wie moet het worden gemeld, hoe moet het worden gemeld, ...). Deze procedure geeft dan aanleiding tot een onderzoek.

Het is evident dat het ontvangen, beheren, analyseren, bestuderen en verwerken van dergelijke meldingen kan en zal resulteren in de verwerking van persoonsgegevens in de zin van de AVG. De regelingen van de professionele interne waarschuwingssystemen moeten bijgevolg in overeenstemming zijn met de AVG.

Zo zal een melding van ongepast gedrag door een collega bv. leiden tot de verwerking door de werkgever van persoonsgegevens van zowel de klokkenluider als de aangeklaagde persoon.

Op dit moment is er nog steeds geen Europese wetgeving die de klokkenluiders officieel beschermt. Het Europees Parlement heeft een richtlijn aangenomen over de bescherming van personen die inbreuken op het recht van de Unie melden, maar die is nog niet in werking getreden. Ze zou uiterlijk op 17 december 2021 worden omgezet. In België bestaat er een bescherming, maar alleen voor werknemers in de federale overheidssector, dankzij de wet van 15 september 2003 betreffende de melding van een veronderstelde integriteitsschending in de federale administratieve overheden door haar personeelsleden. De reikwijdte is dus beperkt.

Bij gebrek aan specifieke wettelijke bepalingen ligt de vrijheid van meningsuiting van de werknemer zodoende in balans met de plicht tot loyaliteit aan de werkgever.

Noodzaak en evenredigheid

Door dit rechtsvacuüm is het des te belangrijker dat de regels voor het instellen van waarschuwingsprocedures worden besproken, anders kunnen deze niet worden ondersteund binnen de organisatie.

De invoering van een dergelijk systeem impliceert een evenwicht waarbij de rechtmatige belangen van alle partijen (de organisatie, de klokkenluider en de aangeklaagde persoon) met elkaar worden verzoend.

In de eerste plaats is het van essentieel belang dat de werkgever een reeks preventieve maatregelen treft om ongepast gedrag van werknemers te voorkomen.

De werkgever moet dus nagaan of de bestaande vormen van toezicht zoals het gebruik van camera's, steekproefsgewijze controles, audits enz. niet reeds voldoende inzicht verschaffen in het niet-conform gedrag van werknemers.

De vraag rijst dan of een beroep doen op werknemers om de beroepsethiek van andere werknemers te controleren noodzakelijk is en, zo ja, of dit evenredig is.

In dit geval wordt de werknemer officieel verzocht deel te nemen aan de logica van de werkgever over de controle van de werknemers. De werknemer kan gevraagd worden tekenen van een niet-integere houding bij zijn eigen collega's op te sporen en te melden. Denk bv. aan kastekorten, kantoorbenodigdheden die verdwijnen, een overdreven aantal gewerkte uren, oneigenlijke onkostenaangiftes enz.

Elke werknemer wordt zo potentieel een controleur en/of wordt potentieel gecontroleerd door andere collega's. Deze manier van werken wekt uiteraard geen sfeer van wederzijds vertrouwen in de hand, noch tussen de werknemers onderling, noch tussen de werknemers en de werkgever. Bovendien moet rekening worden gehouden met de contraproductieve gevolgen die de voorgestelde maatregelen kunnen hebben voor de kwaliteit van de arbeidsrelaties en van het werk zelf.

Aanwerving van kandidaten

De Arbeidsovereenkomstenwet van 3 juli 1978 is van toepassing vanaf de totstandkoming van de overeenkomst. Voorafgaand aan het sluiten van de overeenkomst zijn de partijen er echter aan gehouden verplichtingen na te leven uit andere regelgeving. Daarnaast zijn de partijen verplicht zich tijdens de wervings- en selectieprocedure te houden aan een reeks voorschriften en gedragsregels die zijn vastgelegd in een collectieve arbeidsovereenkomst.

In zijn zoektocht naar de juiste persoon voor de juiste baan probeert de werkgever informatie te verzamelen bij de kandidaat om te beslissen of de man of vrouw wordt aangeworven of afgewezen. De (goedbedoelde) ambitie van de werkgever zoveel mogelijk informatie over de kandidaten te verzamelen kan echter een inbreuk op de privacy inhouden.

Daarom mag de werkgever niet meer persoonsgegevens over de kandidaat verzamelen dan nodig is om zijn doel te bereiken. De vragen mogen alleen betrekking hebben op de aard en de voorwaarden van de functie waarvoor de kandidaat solliciteert. Alleen de persoonsgegevens die strikt noodzakelijk zijn voor de selectie van de kandidaten mogen worden verzameld en geregistreerd.

Een werkgever kan bv. nooit vragen naar een chronologisch overzicht van de privéadressen van een kandidaat, omdat deze informatie geen nut heeft. Alleen het huidige privéadres is relevant.

Vraag over gevoelige gegevens van de sollicitant

De AVG verbiedt in principe de verwerking van gevoelige gegevens.

Het gaat om de volgende categorieën gegevens met betrekking tot:

ras;
politieke overtuigingen;
religieuze of levensbeschouwelijke overtuigingen;
vakbondslidmaatschap;
seksuele gerichtheid.

Dit verbod is gerechtvaardigd gezien de uiterst gevoelige aard van deze gegevens en de mogelijke schade die een ongecontroleerd gebruik van deze gegevens de kandidaat kan toebrengen. Er zijn echter uitzonderingen op dit principiële verbod. De verwerking van dergelijke gevoelige gegevens kan in het kader van de arbeidsrelatie en bij wijze van uitzondering mogelijk zijn wanneer dit voor de werkgever noodzakelijk is om zijn specifieke rechten en plichten op het gebied van het arbeidsrecht te kunnen vervullen.

ETNISCHE REGISTRATIE VAN KANDIDATEN

In het licht van het noodzakelijkheidscriterium kan de werkgever in zijn personeelsbeleid rekening houden met de etnische gegevens van de sollicitanten om voldoende mensen van diverse origine aan te werven, zodat iedereen gelijke kansen krijgt op de arbeidsmarkt. Dergelijke etnische persoonsgegevens mogen vervolgens echter niet worden gebruikt voor een ander doel dan het doel dat wordt beschreven in de wetgeving die de werkgever toestaat etnische persoonsgegevens te verwerken. Bovendien moet de werkgever de kandidaat op de hoogte brengen van de wet waarop hij zich baseert wanneer hij naar zijn etnische afkomst vraagt, vermits er gevoelige persoonsgegevens worden verzameld.

Als de werkgever zich niet op de wetgeving beroept, mag hij alleen etnische gegevens gebruiken als de kandidaat hier uitdrukkelijk mee instemt. In dat geval moet de werkgever de kandidaat vooraf informeren over de redenen waarom hij de etnische afkomst wenst te kennen en wie daarvan later op de hoogte zal worden gebracht.

VRAGEN MET BETREKKING TOT DE POLITIEKE OPVATTINGEN EN RELIGIEUZE OF LEVENSBESCHOUWELIJKE OVERTUIGINGEN VAN DE KANDIDATEN

Vragen met betrekking tot een politieke mening of religieuze overtuiging zijn en blijven een verwerking van gevoelige gegevens en zijn dus in principe verboden.

Er is echter een uitzondering. Het verbod is niet van toepassing als de verwerking plaatsvindt in het kader van een aanwervingsprocedure die wordt uitgevoerd door een vereniging die actief is in de politiek, een vakbond of een ziekteverzekering of als het een religieuze of levensbeschouwelijke instelling betreft. In dat geval is de politieke opinie of de religieuze overtuiging daadwerkelijk verbonden met de aard en de omstandigheden van de functie. Het is bv. niet onlogisch een kandidaat-leraar katholieke godsdienst op een katholieke school te vragen of hij het katholieke geloof aanhangt.

VRAGEN OVER HET LIDMAATSCHAP VAN EEN VAKBOND IN HET KADER VAN EEN KANDIDAATSTELLING

Het lidmaatschap van een vereniging die actief is op het vlak van politiek, levensbeschouwing, godsdienst, ziekteverzekering of vakbond (en de rol die de kandidaat daarin speelt) is ook een gevoelig gegeven. Het is in principe verboden dergelijke gegevens op te vragen en te verwerken, zelfs als de werkgever het sociale engagement van een kandidaat wil kunnen beoordelen. Dit is een onevenredige inbreuk op de privacy van de kandidaat.Als de werkgever een toonaangevende organisatie is (bv. een politieke partij, een vakbond, een ziekteverzekering enz.), is het verzoek om deze gegevens en de eventuele verwerking ervan toch verdedigbaar. Dergelijke organisaties – gedreven door een duidelijke vakbonds-, politieke of religieuze visie – kunnen van hun leden eisen dat ze trouw zijn aan hun principes. Ze kunnen op zijn minst vragen of proberen te achterhalen of de kandidaat hun vakbonds-, politieke of religieuze beginselen onderschrijft.

Vragen over de gezondheid en medische gegevens van de sollicitant

Het is niet toegestaan een kandidaat te ondervragen over zijn gezondheidstoestand, tenzij voor specifieke functiekenmerken nog informatie over de gezondheidstoestand van de kandidaat nodig is om de geschiktheid van de kandidaat te beoordelen.

Dit kan het geval zijn als een medische aandoening de veiligheid van de werknemer, collega's of derden in gevaar kan brengen (een lijnpiloot is bv. best niet slechtziend).

Voor bepaalde functies, zoals een politieagent, omvat de selectieprocedure een gezondheidsevaluatie. Deze gezondheidsevaluatie vindt echter pas plaats aan het einde van de selectieprocedure en kan niet worden gebruikt om een keuze te maken. Het spreekt voor zich dat ook hier alleen rekening kan worden gehouden met gezondheidsgegevens die verband houden met de uitvoering van de specifieke functie.

Als een werkgever een geneeskundig onderzoek wil laten uitvoeren, is de AVG van toepassing. Het (laten) verrichten van een medisch onderzoek is immers een manier om informatie over de kandidaat te verzamelen en vormt dus een verwerking van persoonsgegevens.

In deze situatie is het de bedoeling gezondheidsgerelateerde gegevens en hun mogelijke invloed op de arbeidsprestaties te beoordelen. Omdat de verwerking van gegevens met betrekking tot de gezondheid in principe verboden is, mag een werkgever een kandidaat alleen vragen een medisch onderzoek te ondergaan als hij gebruik kan maken van een van de uitzonderingen die in de Kaderwet worden genoemd.

Een van deze uitzonderingen is de schriftelijke toestemming van de kandidaat. Een andere uitzondering is de noodzaak van de verwerking om te voldoen aan de specifieke rechten en plichten van de werkgever op het vlak van het arbeidsrecht.Een kandidaat vragen of ze zwanger is of vragen naar haar kinderwens is verboden omdat de werkgever deze informatie bij de meeste vacatures niet nodig heeft om een selectie te maken. Dergelijke vragen kunnen bij uitzondering toegestaan zijn als de in te vullen functie een gevaar vormt voor het ongeboren kind.

Vragen over het gerechtelijke verleden van de sollicitant

Volgens de AVG zijn dergelijke vragen in principe verboden.

Als het echter een beroep betreft waarvoor de wet vereist dat de houder over een blanco strafblad beschikt of niet veroordeeld mag zijn voor bepaalde zaken, kunnen deze vragen toch worden gesteld. In dat geval zijn ze namelijk noodzakelijk voor de correcte toepassing van deze wet. We denken hier bv. aan een politieagent of het personeel van een bewakingsbedrijf.

In dat geval moet de werkgever, zodra hij weet dat de kandidaat voldoet aan de integriteitsvereisten voor de vacante functie (omdat hem een uittreksel uit het strafregister is overhandigd), beslissen of hij al dan niet tot de aanwerving overgaat. Hij heeft er echter geen belang bij deze persoonsgegevens achteraf te bewaren.De verwerking (bv. het bewaren) van dergelijke gegevens is alleen mogelijk in een aantal gevallen die in artikel 10 worden genoemd. De toestemming van de kandidaat vormt in ieder geval geen rechtsgrond voor de verwerking van dergelijke persoonsgegevens.

Verzameling van gegevens van de kandidaat bij vorige werkgevers en klanten: onderzoek van referenties

Persoonsgegevens moeten in principe van de kandidaat zelf worden verkregen.

Als de werkgever echter informatie wenst te verkrijgen van derden, als verwerkingsverantwoordelijke, zal hij de toestemming van de kandidaten moeten krijgen om:

hun gegevens te verzamelen,
deze gegevens te verwerken voor wervingsdoelen (machtiging voor verwerkers die namens de werkgever optreden).

Daarnaast moet de werkgever de kandidaten ook altijd op de hoogte stellen wanneer hij informatie over hem opvraagt bij derden (dus zelfs als de kandidaat zijn toestemming heeft gegeven).

Volgens de AVG moet deze toestemming vrij zijn. Dit is niet het geval als de selectieprocedure wordt stopgezet of als de kandidaat een onderzoek van referenties weigert. Dit is een wettelijke 'instemmingsplicht'.

De kandidaat geeft zijn toestemming door een verklaring te ondertekenen waarvan hij de draagwijdte duidelijk kan begrijpen en die ten minste de volgende verklaringen bevat:

zijn identiteit en de identiteit van de organisaties of de personen die de werkgever wil raadplegen;
de aard van de gevraagde gegevens;
de redenen voor het verzamelen van de gegevens;
de periode waarin de toestemming zal worden gebruikt.

Als een referentiepersoon in het cv wordt vermeld, kan dit gelden als een toestemming van de kandidaat.

In ieder geval mag de werkgever de informatie die de kandidaat aan hem heeft doorgegeven niet systematisch bij derden controleren.Als een cv duidelijk hiaten vertoont, moet de werkgever de kandidaat eerst zelf vragen naar deze duidelijke 'lacunes' in zijn opleidings- en loopbaantraject. Pas dan, als de uitleg van de kandidaat over het onderwerp niet afdoende was, kan de potentiële werkgever overwegen gegevens van andere personen of organisaties te verzamelen, op voorwaarde dat de kandidaat daarvan vooraf op de hoogte is gesteld en daarvoor zijn toestemming heeft gegeven.

Bij geautomatiseerde persoonlijkheids- of psychotechnische tests moet er altijd een procedure zijn om de kandidaat zijn mening over de verkregen resultaten te laten kenbaar maken.

De AVG verbiedt immers een beslissing met juridische gevolgen te nemen ten aanzien van de kandidaat of een beslissing met een beduidende impact voor hem, bv. het besluit hem in dienst te nemen, uitsluitend op basis van een geautomatiseerde gegevensverwerking.

Selectiebureaus

Het selectiebureau bepaalt op verzoek van een werkgever de geschiktheid van de kandidaten voor een bepaalde functie door middel van gesprekken en psychologische tests. In dat verband spreekt het voor zich dat een selectiebureau persoonsgegevens van sollicitanten verwerkt. Het selectiebureau moet dus voldoen aan de AVG zonder de specifieke wetgeving met betrekking tot de selectiebureaus uit het oog te verliezen.

VERZAMELING VAN PERSOONSGEGEVENS VAN KANDIDATEN

De naleving van de AVG houdt met name in dat als het selectiebureau een dossier van een kandidaat samenstelt, dit dossier niet meer gegevens mag bevatten dan nodig is voor de vacante functie. Bijgevolg kan niet voor elke vacature dezelfde vragenlijst worden gebruikt, omdat voor de ene functie bepaalde gegevens nodig zijn en voor de andere functie andere. Bovendien kan het selectiebureau de kandidaat alleen om persoonsgegevens vragen als dit noodzakelijk is voor de werksituatie.

Vragen met als doel de opeenvolgende verblijfplaatsen van een kandidaat te weten te komen zijn niet relevant. Vragen in wat voor soort woning hij woont of dat hij een huurder of een verhuurder is, lijken meer een kwestie van nieuwsgierigheid dan van noodzaak.

Bovendien mag een selectiebureau geen vragen stellen die tot discriminatie van de kandidaat kunnen leiden. Het selectiebureau mag geen onderscheid maken op basis van leeftijd, seksuele geaardheid, godsdienstige of levensbeschouwelijke overtuiging of handicap, enkel op basis van essentiële en bepalende beroepsvereisten.

RAADPLEGING VAN HET DOSSIER VAN DE KANDIDAAT

Daarnaast heeft de kandidaat het recht de persoonlijke resultaten van zijn interviews, tests en praktijkexamens in te kijken. Algemene gegevens die niet specifiek de kandidaat betreffen, zoals de voorgestelde en uitgewerkte algemene richtlijnen voor de resultaten, de geldigheid en de interpretatie van psychologische tests en de correcte antwoorden op objectieve tests, vallen niet onder het raadplegingsrecht.

Dit raadplegingsrecht biedt de kandidaat de mogelijkheid zijn recht op rechtzetting uit te oefenen.

Als een kandidaat zich beroept op het recht een kopie van het dossier te krijgen, wordt in de rechtsleer aanvaard dat dit geen algemene verslagen of testresultaten omvat die door het selectiebureau zijn opgesteld. De kandidaat kan dit recht doen gelden op basis van de specifieke regelgeving van de selectiebureaus en niet op basis van de Kaderwet, die alleen voorziet in een raadplegingsrecht.

RECHTZETTING VAN HET DOSSIER

Volgens de AVG kan elke persoon gratis de correctie van onjuiste persoonsgegevens bekomen.

De kandidaat kan ook zijn recht op rechtzetting uitoefenen in verband met de evaluatie als hij het er niet mee eens is. Dit betekent niet dat hij dan zijn eigen beoordeling kan vervangen, maar hij kan wel aangeven dat hij het er niet mee eens is. Een 'slechte' evaluatie van de kandidaat immers in diskrediet brengen.

BYOD

Werkgevers worden geconfronteerd met een toenemende aanwezigheid van smartphones en tablets op de werkplek. Dat stelt hen voortdurend voor nieuwe managementuitdagingen. Als de werkgever deze apparaten zelf beschikbaar stelt aan werknemers, wordt dit Mobile Device Management (MDM) genoemd. De werkgever krijgt echter steeds vaker verzoeken van medewerkers om hun eigen smartphone of tablet op de werkplek te mogen gebruiken. In dit geval heet het BYOD (Bring Your Own Device).

Het gebruik van mobiele apparaten in een professionele context

Het gebruik van mobiele apparaten heeft vele voordelen (al was het maar om het verslag van de vergadering ter plaatse te schrijven of het internet te raadplegen). Het heeft echter ook nadelen. Het gebruik van mobiele apparaten brengt specifieke risico's met zich mee voor de informatiebeveiliging en de privacy door hun belangrijkste troef, namelijk hun draagbaarheid.

Informatie over het bedrijf en persoonsgegevens over werknemers kan worden verspreid na een de diefstal van mobiele apparaten of via het onderscheppen van gegevens bij het gebruik van openbare wifitoegangspunten. Deze apparaten kunnen ook, bewust of onbewust, worden gebruikt om kwaadaardige software (malware) in het bedrijfsnetwerk te introduceren.

Ten slotte vereist het feit dat deze apparaten zich over het algemeen dicht bij de eigenaar bevinden en dat ze vaak 24 uur per dag actief zijn, bijzondere aandacht voor het beschermingsniveau van de persoonsgegevens van de gebruiker en, meer specifiek, voor de geolocatie van de werknemers.

BYOD

Het gebruik van de eigen apparaten door werknemers, zowel voor privé- als voor professioneel gebruik, maakt de kwestie van het toezicht op de apparaten door de werkgever en de gegevens die ze bevatten complex. Sinds de inwerkingtreding van de AVG is de werkgever verplicht de

veiligheid van de persoonsgegevens van zijn bedrijf te waarborgen, ook wanneer deze zijn opgeslagen op terminals waarover hij geen fysieke of juridische controle heeft.

In dit geval is de uitoefening van het evenwicht tussen de verdediging van het rechtmatig belang van de werkgever om controle uit te oefenen en het behoud van de fundamentele rechten en vrijheden met betrekking tot de bescherming van de privacy van de werknemer niet altijd eenvoudig.

Enerzijds heeft de werkgever het recht controle uit te oefenen op de bedrijfsgegevens op de BYOD-apparaten. Deze controle is noodzakelijk om de veiligheid en vertrouwelijkheid van deze bedrijfsgegevens (bv. klantenbestanden) te waarborgen.

In de BYOD-situatie moet de werkgever maatregelen treffen om de bedrijfsgegevens te beschermen (en de persoonsgegevens van zijn klanten) op het BYOD-apparaat, die door de werknemer voor professionele doeleinden worden gebruikt en verwerkt.

Deze controlemogelijkheid voor de werkgever houdt in dat de werknemer de professionele gegevens op zijn BYOD-apparaat niet te kwader trouw mag achterhouden of aan de raadpleging door de werkgever mag onttrekken. De werkgever moet de gegevens en apparaten kunnen controleren op mogelijk misbruik, ook al zijn de gegevens in een BYOD-apparaat ten minste gedeeltelijk ook van persoonlijke aard, gezien het apparaat eigendom is van de werknemer en dus per definitie ook bedoeld is voor privégebruik door de betrokken werknemer en/of door derden (bv. zijn gezinsleden).

Anderzijds heeft de werknemer ook recht op privacy. Gezien een BYOD-apparaat per definitie zowel professionele als persoonlijke doeleinden dient, doet zich ook een probleem voor op het vlak van de privacy. Het gezag van de werkgever volstaat niet om alle informatie op BYOD-apparaten zonder meer te controleren. Er moeten specifieke maatregelen worden getroffen om de persoonsgegevens te beschermen door deze te isoleren van de zakelijke gegevens.