UZ LEUVEN | ALGEMENE DIRECTIE

Policy voor meldingen van inbreuken op het Unierecht (*Klokkenluidersregeling*)

1. Situering

Dit document omschrijft de procedure voor de melding van inbreuken in UZ Leuven zoals bepaald in de Wet betreffende de bescherming van melders van inbreuken op het Unie- of nationaal recht vastgesteld binnen de juridische entiteit in de private sector en is een onderdeel van het globale beleid waarmee de organisatie een open en integere bedrijfscultuur nastreeft.

Deze wet schrijft voor dat een melder in een werkgerelateerde context op een veilige, vertrouwelijke en, indien gewenst, ook anonieme wijze een melding moet kunnen maken van inbreuken op essentiële beleidsterreinen. Deze melding kan zowel gebeuren via een meldkanaal opgezet door de UZ Leuven als via een extern meldkanaal. Inbreuken omvatten zowel onrechtmatige handelingen of nalatigheden, als misbruik.

UZ Leuven voorziet in een eigen meldkanaal via een elektronische tool en garandeert dat de behandeling van dergelijke meldingen op een ernstige en discrete wijze gebeurt binnen de voorgeschreven termijn.

UZ Leuven verwijst daarnaast naar de mogelijkheid om een melding te doen bij het extern meldkanaal van de overheid (bij de federale Ombudsman) – al dan niet tezamen met een melding bij het intern meldkanaal.

Van alle betrokkenen wordt verwacht dat zij deze meldingsprocedure op een correcte en respectvolle manier toepassen.

2. Toepassingsgebied: wie kan melden?

Een "melder" is elkeen die bij UZ Leuven werkzaam is of is geweest of werkzaamheden heeft verricht in welke hoedanigheid dan ook: werknemers, zelfstandigen, interims of consultants, bestuurders, leidinggevenden, maar ook vrijwilligers, stagiairs en eenieder die werkt onder toezicht en leiding van aannemers, onderaannemers en leveranciers van UZ Leuven.

Ook personen van wie de werkrelatie nog moet aanvatten, kunnen ingeval van informatie over inbreuken verkregen tijdens de wervingsprocedure of andere precontractuele onderhandelingen een beroep doen op deze meldprocedure.

3. Begrip "meldingen"

3.1. Meldingen waarop de policy van toepassing is

Alle informatie over feitelijke of mogelijke inbreuken die hebben plaatsgevonden of zeer waarschijnlijk zullen plaatsvinden binnen de organisatie waarvan de melder kennis heeft binnen een werkgerelateerde context, met inbegrip van (zonder exhaustief te zijn):

- Overheidsopdrachten;
- Financiële diensten;
- Producten en markten;
- Voorkomen van het witwassen van geld en de financiering van terrorisme;
- Productveiligheid en productconformiteit;
- Veiligheid van het vervoer;
- Bescherming van het milieu;
- Stralingsbescherming en nucleaire veiligheid;
- Veiligheid van levensmiddelen, dierenvoeding en - gezondheid en dierenwelzijn;
- Volksgezondheid;
- Consumentenbescherming;
- Bescherming van persoonlijke levenssfeer en persoonsgegevens en beveiliging van netwerk- en informatiesystemen;
- Bestrijding van belastingfraude;
- Sociale fraudebestrijding;
- Financiële belangen van de EU;
- Verstoring van de interne markt.

De meldingen hebben betrekking op inbreuken die in hoofdzaak het algemeen belang schaden of bedreigen.

3.2. Meldingen waarop de policy niet van toepassing is

De policy is niet van toepassing op andere domeinen dan hierboven gemeld, en dus o.m. niet op persoonlijke, werkgerelateerde bekommernissen zoals ontevredenheid over lonen, werktijden, werkplaatsomstandigheden, interpersoonlijke problemen en/of prestatiebeoordelingen, een arbeidsongeval, grensoverschrijdend gedrag, …

Voor deze aangelegenheden gelden de reeds bestaande meldkanalen en procedures en kan de werknemer terecht bij desbetreffende kanalen.

4. Procedure meldkanaal

4.1. Voorafgaandelijk

Wie op grond van deze policy een aangifte doet, moet een gegronde reden hebben die aantoont dat de gemelde informatie over de inbreuken op het moment van de melding juist is, handelt over een materie die valt binnen het toepassingsgebied vermeld onder 3.1. en de inbreuk kunnen staven met objectieve, ondersteunende informatie.

Elke melder moet te goeder trouw optreden. Een medewerker die opzettelijk valse informatie meldt of openbaar maakt kan gesanctioneerd worden op basis van de maatregelen opgenomen in het arbeidsreglement/de algemene regeling of kan strafrechtelijk vervolgd worden.

De melder kan naar goeddunken beslissen of hij/zij al dan niet anoniem wenst te blijven. Ingeval de melding anoniem gebeurt dan kan dit evenwel een impact hebben op de kwaliteit van het onderzoek en het niveau waarop dit kan worden gevoerd, of kan verder onderzoek zelfs onmogelijk maken.

Om de kwaliteit van het onderzoek en het niveau waarop deze materie behandeld kan worden te verhogen is het van het grootste belang dat de melder zoveel mogelijk voorafgaandelijke informatie verzamelt over de inbreuk.

De melder kan een inbreuk melden via het meldkanaal dat door UZ Leuven is voorzien (zie verder punt 4.2.) ofwel rechtstreeks (al dan niet parallel aan de melding bij het voorvermeld meldkanaal), aangeven bij het extern meldkanaal dat door de overheid is opgericht, m.n. bij de federale ombudsman (zie voor meer informatie: https://www.federaalombudsman.be/nl/klokkenluiders).

4.2. Het meldkanaal opgezet door UZ Leuven

UZ Leuven beschikt over een eigen beveiligd en vertrouwelijk kanaal voor meldingen. Indien een melding onder het toepassingsgebied van de policy valt, dan maakt de melder dit via dit kanaal bekend.

UZ Leuven maakt gebruik van de tool die door de FOD WASO werd aanbevolen en die ontwikkeld werd door Globaleaks. De link naar deze tool is terug te vinden op de website van UZ Leuven.

Deze gecentraliseerde meldingstool stelt UZ Leuven in staat om zicht te krijgen op het aantal en het type meldingen en maakt als dusdanig een objectieve rapportering mogelijk.

4.3. Verdere behandelingen en onderzoek van de meldingen

Wanneer een melding via de meldingstool gedaan wordt, ontvangt de melder automatisch een bevestiging van de melding via de tool.

Alle meldingen die in de meldingstool binnenkomen, worden door UZ Leuven in overeenstemming met de hiernavolgende procedure behandeld:

- De interne preventieadviseur die in deze procedure optreedt als procesbeheerder, voert in samenspraak met de personeelsdirecteur en de algemeen secretaris een eerste screening uit van de melding. Zij verifiëren of de melding binnen het toepassingsgebied van de policy valt.

- Als dit het geval is, dan wordt de melding doorgestuurd naar een onderzoeksteam met de vraag om samen te komen om de betreffende melding te onderzoeken. Dit onderzoeksteam bestaat uit de procesbeheerder en de HR-directeur waaraan, afhankelijk van de aard van de gerapporteerde problemen en de betrokken afdeling andere experten worden toegevoegd. Indien een lid een belangenconflict heeft, wordt deze uitgesloten van verdere deelname aan het onderzoek om de nodige objectiviteit te waarborgen.

- Het onderzoeksteam controleert de gegrondheid van de melding en gaat na welke gepaste maatregelen kunnen genomen worden: een intern vooronderzoek, een onderzoek, klacht indienen, terugvordering van middelen, het beëindigen van de procedure.

- De melder krijgt binnen de 7 werkdagen een ontvangstbevestiging van het onderzoeksteam. Ook indien de melding buiten het toepassingsgebied van de policy valt, wordt de melder hiervan binnen deze termijn op de hoogte gebracht en aangemoedigd om het gemelde probleem aan te kaarten bij het meest geëigende meldingskanaal, rekening houdend met de aard van de melding.

- Het onderzoeksteam onderzoekt het dossier in nauw overleg met de melder.
    - Indien de melder zijn identiteit heeft bekendgemaakt, dan verloopt de communicatie met het onderzoeksteam via mail, telefoon, …
    - Indien de melder zijn melding anoniem heeft gedaan, dan verloopt de communicatie met het onderzoeksteam via de beveiligde mailbox van de meldingstool.

- De melder wordt in ieder geval binnen de 3 maanden vanaf de datum waarop het onderzoeksteam aan de zaak werd toegewezen, op de hoogte gebracht van de ontwikkelingen in het onderzoek.

- Afhankelijk van de melding kan het nodig zijn om externe consultants bij het onderzoeksproces te betrekken. Indien zich een strafrechtelijk misdrijf heeft voorgedaan, kunnen ook politiediensten hierbij betrokken worden.

- Zodra het probleem behandeld en opgelost is, worden de persoonsgegevens die in de melding zijn opgenomen geanonimiseerd en wordt het dossier gearchiveerd zonder inbreuk te doen aan de verplichtingen van de GDPR.

5. Bescherming van de melder

5.1. Niet-bekendmaking

De meldingsprocedure garandeert in de mate van het mogelijke dat de identiteit van de melder niet onthuld wordt.

De leden van het onderzoeksteam zijn verplicht om de confidentialiteit in acht te nemen. UZ Leuven kan evenwel tijdens het onderzoek wettelijk verplicht zijn om de informatie die verworven is kenbaar te maken aan de bevoegde overheidsinstanties (o.a. ingeval van strafrechtelijke misdrijven).

5.2. Bescherming tegen represailles

Een melder geniet van een beschermd statuut en mag dus niet ontslagen, geschorst, bedreigd, geïntimideerd of het slachtoffer van represailles worden als gevolg van het feit dat hij te goeder trouw bepaalde feiten heeft gemeld.

Bij anonieme melding geldt de bescherming als de melder zich identificeert.

De personen die een actieve ondersteuning geven aan de melder tijdens de meldprocedure of familieleden van de melder genieten van dezelfde bescherming.

Klachten in verband met represailles tegen de melder worden onmiddellijk geverifieerd en indien nodig onderzocht.

Indien een melder bewust een valse verklaring heeft geuit, tijdens het onderzoek valse of misleidende informatie heeft verstrekt of op enige andere wijze te kwader trouw gehandeld heeft, kan hij hiervoor gesanctioneerd en/of strafrechtelijk vervolgd worden.

6. Gegevensbescherming

Elke verwerking van de melding gebeurt in overeenstemming met de GDPR. Niet gemachtigde personen hebben geen toegang tot de gegevens. Het register van elke ontvangen melding beantwoordt aan de geheimhoudingsvereisten en de meldingen worden niet langer opgeslagen dan noodzakelijk en zijn evenredig voor het onderzoek en de remediëring van de melding.

7. Rapportering

De meldingsdienst maakt eenmaal per jaar een verslag op over de werking dat ter validatie wordt voorgelegd aan de CEO. Het DC ontvangt dit jaarverslag ter informatie. Het bestuursorgaan ontvangt jaarlijks een samenvatting van voornoemd jaarverslag.