BELEID

Juridische dienst
T 056 62 98 47
privacy@waregem.be

Aan	**Ref**	**Contactpersoon**	**Waregem**
		Carmen Vandemaele	goedgekeurd op 29 maart 2022

Logbeleid

Inhoudstafel.

1. Inleiding.

Informatiesystemen en ICT-infrastructuur genereren loginformatie voor veel activiteiten, soms als normale statusmelding, soms als resultaat van een activiteit van een gebruiker of beheerder maar ook informatie als resultaat van onvoorziene omstandigheden of fouten. Een log beschrijft wat er gebeurt binnen systemen.

Via het logbeleid wil het lokaal bestuur Waregem duidelijke regels vastleggen omtrent toegang, gebruik en bescherming van privacy logs. Privacy logs zijn logs aangemaakt om te voldoen aan en te beantwoorden op privacy regelgeving. Privacy logs dienen minstens 10 jaar bewaard te worden.

2. Scope van het beleid.

Dit beleid geldt voor:

- alle personeelsleden van de organisatie, zowel interne als externe medewerkers, met inbegrip van het personeel dat ter beschikking gesteld wordt, zowel voor onbepaalde als bepaalde duur (bv. consultants, leveranciers, …);
- alle natuurlijke personen of rechtspersonen die gebruik maken van of toegang krijgen tot persoonsgegevens, al dan niet voor rekening van het lokaal bestuur;
- alle persoonsgegevensverwerkende systemen;
- alle verwerkingsactiviteiten m.b.t. persoonsgegevens.

3. Beleidsrichtlijnen rond privacy logs.

- Inhoud van privacy logs

  De privacy logs van het bestuur moeten volgende vragen kunnen beantwoorden:
  - Welke activiteit had plaats? (wat)
  - Wanneer gebeurde de activiteit? (wanneer)
  - Wie voerde de activiteit uit? (wie)
  - Met welk systeem gebeurde de activiteit? (hoe)
  - Om welke betrokkene gaat het? (over wie)
  - Wat was het resultaat van de activiteit? (gelukt/niet gelukt)

  Dit betekent dat de inhoud van de logs minstens bestaat uit de volgende velden/vermeldingen per activiteit die gelogd wordt:
  - De datum en het uur van de transactie (timestamp).
  - De identificatie van de gebruiker (naam, nummer, username,…).
  - De identificatie van de transactie (opeenvolgende nummering).
  - De identificatie van het onderwerp van de transactie (welke patiënt, cliënt, etc.).
  - De beschrijving van de uitgevoerde bewerking (create-read-update-delete).

- Toegang tot logbestanden

  Logbestanden dienen beschermd te worden tegen inzage door onbevoegden, wijzigingen en verwijderingen. Bijgevolg wordt de raadpleging van logs strikt beperkt. Behoudens afwijkende instructies van de algemeen directeur, heeft enkel de DPO toegang tot privacy logs. De toegang tot logbestanden, vereist een sterke authenticatie. Bij sommige toepassingen hebben medewerkers zelf de toegang tot de recentste logs.

Onderzoek van de privacy logs gebeurt door de DPO op het uitdrukkelijke verzoek van :

- De kamer van sociale zekerheid en gezondheid van het informatieveiligheidscomité;
- De algemeen directeur;
- De inspectiediensten;
- De DPO in het kader van zijn periodiek wettelijk verplichte controles;
- De burger, bewoner, cliënt, … of diens wettelijk vertegenwoordiger.

Personeelsleden die in het kader van toegangsbeheerder van een softwarepakket toegang hebben tot logbestanden, dienen zich te houden aan de gedragscode voor informatiebeheerders zoals gedefinieerd in bijlage C van het *beleidslijn Gedragscode voor informatiebeheerders* van de Minimale Normen KSZ.

- Logregister

Het bestuur houdt een register bij van de verzoeken die werden goedgekeurd/uitgevoerd of die werden afgekeurd met betrekking tot privacy logs. Het logregister wordt up tot date gehouden door de DPO.

- Resultaten van de controle.

Het resultaat van logbeheer wordt gerapporteerd en besproken binnen de Informatieveiligheidscel. Bij vaststellingen van onregelmatigheden kunnen er disciplinaire maatregelen genomen worden conform de geldende wetgeving en arbeidsreglement.

- Aankoop nieuwe software en vereisten van de logbestanden.

Logbeheer moet meegenomen worden vanaf het design tijdens de ontwikkeling of bij de bepalingen van aankoopcriteria van toepassingen of systemen om “security/privacy by design” te realiseren.

Personeelsleden die instaan voor de aankoop van hard-en software dienen ervoor in te staan dat het logbeheer meegenomen wordt bij de aankoopcriteria. Hierbij dient volgend principe toegepast te worden: elke toegang tot gegevens met gevoeligheidsklasse vertrouwelijk of hoger, moet gelogd worden in overeenstemming met de toepasselijke regelgeving en het intern logbeleid.

- Synchronisatie van systeemklokken.

De dienst ICT ziet erop toe dat systeemklokken zodanig gesynchroniseerd zijn zodat altijd een betrouwbare analyse van logbestanden mogelijk is.

- Informatieplicht

Medewerkers zijn via het arbeidsreglement en algemene sensibilisering Informatieveiligheid geïnformeerd over de mogelijkheid van het bestuur om logs te controleren.