



**RAAD VAN
DE EUROPESE UNIE**

**Brussel, 11 juni 2003 (17.06)
(OR. en)**

10040/03

LIMITE

EUROPOL 38

NOTA

van: Europol
aan: het Comité van artikel 36/het COREPER/de Raad
Betreft: Verslag inzake gegevensbescherming: Malta

Voor de delegaties gaat hierbij het door Europol opgestelde verslag inzake gegevensbescherming over Malta, met inbegrip van het advies van het Gemeenschappelijk Controleorgaan van Europol.

Verslag inzake gegevensbescherming: Malta

1. INLEIDING EN ALGEMENE OVERWEGINGEN

Op 27 maart 2000 heeft de Raad een verklaring aangenomen betreffende de betrekkingen van Europol met derde staten en niet aan de Europese Unie gerelateerde instanties, met name met betrekking tot de verstrekking van persoonsgegevens door Europol aan derde staten en instanties. Teneinde het de Raad mogelijk te maken na te gaan of er eventuele hindernissen overwonnen dienen te worden voor het begin van dergelijke onderhandelingen met een bepaalde staat of instantie, wordt de raad van bestuur verzocht om verslagen aan de Raad voor te leggen over de wetgeving en de bestuursrechtelijke praktijken in die derde staat of instantie, met inbegrip van alle voorzieningen voor een onafhankelijk controleorgaan. In dit opzicht is de verklaring in overeenstemming met de in artikel 3, lid 3, vastgelegde regel, in combinatie met artikel 2, lid 2, van het besluit van de Raad van 12 maart 1999, houdende vaststelling van de regels betreffende de verstrekking van persoonsgegevens door Europol aan derde staten en instanties.

Benadrukt moet worden dat al deze verslagen niet bedoeld zijn om een definitief of volledig oordeel te geven over de stand van zaken betreffende de bestuursrechtelijke praktijk inzake gegevensbescherming in een bepaalde staat of organisatie. Hiervoor gelden verscheidene redenen:

- allereerst moet rekening worden gehouden met het doel van de verslagen. Ze worden opgesteld om de Raad te helpen tot een zeer specifiek besluit te komen: is de stand van zaken betreffende gegevensbescherming in een bepaalde derde staat of instantie zodanig dat **begonnen** kan worden met onderhandelingen over de verstrekking van persoonsgegevens door Europol? De verslagen zijn derhalve niet bedoeld om een definitief oordeel te geven over de vraag of al dan niet alle persoonsgegevens onder alle omstandigheden kunnen worden verstrekt;
- ten tweede is het toepassingsgebied van de verslagen uiteraard beperkt. Het is natuurlijk onmogelijk om goed onderzochte, diepgaande verslagen over een dergelijk breed onderwerp in een zo korte tijd en met de ter beschikking gestelde middelen te leveren;

- ten derde verschaffen deze verslagen alleen een momentopname van de situatie. De situatie kan met name ten aanzien van de bescherming van door Europol verstrekte gegevens anders zijn zodra een samenwerkingsovereenkomst is bereikt. In feite zouden de verslagen Europol moeten helpen om gebieden vast te stellen die speciale aandacht vragen, of waarvoor aanvullende beschermende maatregelen in de overeenkomsten opgenomen moeten worden, met andere woorden: bepaalde zwakke punten kunnen worden verholpen door middel van goed opgestelde samenwerkingsovereenkomsten;
- ten vierde verschaft de Europol-Overeenkomst zelf de regel dat beoordeling van de vraag of de mate van gegevensbescherming adequaat is, niet alleen moet worden gebaseerd op de voor de derde staat of instantie geldende algemene of bijzondere voorschriften, maar eveneens op de aard van de gegevens, het doel waarvoor de gegevens worden gebruikt en de duur van de beoogde verwerking.

Het huidige rapport behandelt met name de situatie in Malta. De auteurs willen de Maltese instanties, met name de afgevaardigden van het ministerie van Binnenlandse Zaken en de Maltese politie graag bedanken voor hun samenwerking bij de opstelling van het verslag.

2. JURIDISCH KADER

2.1. Status van een samenwerkingsovereenkomst met Europol

Een samenwerkingsovereenkomst tussen Malta en Europol vereist een ratificatie vóór de inwerkingtreding hiervan. Het is derhalve noodzakelijk dat het Parlement de ratificatie van de overeenkomst toestaat of goedkeurt via een resolutie van het huis van afgevaardigden. De Maltese instanties hebben meegedeeld dat deze procedure, na introductie in het Parlement, in gebruikelijke omstandigheden slechts enkele dagen in beslag neemt. Na de ratificatie van de overeenkomst is deze onmiddellijk van toepassing tenzij de nationale wetgeving moet worden gewijzigd. De Maltese instanties hebben tevens vermeld dat zij dit evenmin verwachten.

2.2. Wetgeving inzake gegevensbescherming in het algemeen

Wat betreft internationale rechtsmiddelen heeft Malta op 15 januari 2003 Verdrag nr. 108 van de Raad van Europa van 1981 tot bescherming van personen ter zake van de geautomatiseerde verwerking van persoonsgegevens ondertekend, maar de ratificatieprocedure is nog niet afgerond. Deze zou naar verwachting worden afgerond in het eerste kwartaal van dit jaar en de inwerkingtreding is drie maand later gepland.

Op het gebied van nationale wetgeving heeft Malta algemene wetgeving op het gebied van gegevensbescherming ingevoerd via de op 14 december 2001 goedgekeurde wet inzake gegevensbescherming van 2001 (wet XXVI van 2001). In deze op 22 maart 2002 in werking getreden wet zijn bepalingen opgenomen over de functionaris voor gegevensbescherming. Deze wetgeving werd goedgekeurd om te voldoen aan de in Richtlijn 95/46/EG vastgestelde normen. Zoals bepaald onder punt 2.3 is deze wetgeving echter niet in zijn geheel van toepassing op gegevensverwerking door politieke autoriteiten, die afzonderlijk is geregeld. Het recht op bescherming van de persoonlijke levenssfeer wordt eveneens vermeld in artikelen 32c en 38 van de Maltese grondwet.

Overige rechtsmiddelen die verband houden met de opslag en verspreiding van gegevens zijn:

- het wetboek voor strafrecht waaruit blijkt dat iedere overheidsfunctionaris een misdrijf pleegt indien hij een hem ambtshalve toevertrouwd of bekend, geheim document of feit openbaar maakt. Dit geldt tevens voor de openbaarmaking van een geheim door eenieder die op grond van zijn vak, beroep of werk, de bewaarder hiervan is;
- de beschikking inzake dienstgeheimen bepaalt dat (voormalige) ambtenaren of overheidscontractanten een misdrijf plegen indien zij zonder toestemming informatie, documenten of dergelijke verspreiden waarvan zij in bezit zijn of waren door de uitoefening van zijn functie en waarvan de verspreiding onder andere de preventie of opsporing van misdrijven of de aanhouding of vervolging van verdachten verhindert of die van dien aard is dat de ongeautoriseerde openbaarmaking hiervan de oorzaak zou kunnen zijn van een van voornoemde gevolgen;
- de wet inzake het beroepsgeheim, die de begrippen “geheim” en “beroepsgeheim” definieert en vastlegt in welke omstandigheden en op welke manier deze openbaar mogen worden gemaakt;
- de wet inzake veiligheidsdiensten die onder andere de vergaring van informatie door de veiligheidsdienst regelt en de niet-openbaarmaking van dergelijke informatie tenzij deze is vereist voor de deugdelijke uitoefening van de taken van de dienst of in het kader van strafrechtelijke vervolgingen.

2.3. Rechtsgrondslag voor gegevensverwerking bij de politie

Artikel 5 van de wet inzake gegevensbescherming van 2001 stelt dat de wet niet van toepassing is op gegevensverwerking met betrekking tot openbare veiligheid, defensie, staatsveiligheid en staatsactiviteiten op het gebied van strafrecht op voorwaarde dat de minister, na overleg met de functionaris en in overeenstemming met de voor de politie verantwoordelijke minister, via regelgevingen bepalingen kan goedkeuren ter uitbreiding van de toepassing van deze wet of ter toevoeging of afwijking van de bepalingen van dit sub-artikel met het oog op de naleving van de bepalingen van een internationale verplichting, overeenkomst of verdrag op het gebied van de bescherming van persoonsgegevens waarvan Malta deel uitmaakt of kan deel uitmaken.

De Maltese instanties hebben artikel 5 aangewend voor de invoering van de regeling inzake gegevensbescherming van 2002 (de verwerking van persoonsgegevens in de politiesector), hierna de regeling inzake gegevensbescherming genaamd. Deze regeling is nog niet van kracht, maar wordt naar verwachting later dit jaar bekend gemaakt. De Maltese instanties hebben te kennen gegeven dat deze regeling is gebaseerd op de bepalingen van aanbeveling R(87)15 van het comité van ministers van de lidstaten van de Raad van Europa tot regeling van het gebruik van persoonsgegevens op politieel gebied.

3. GEGEVENSBECHERMINGSPRINCIPES

Naast de algemene regels inzake de bescherming van gegevens werden ter voorbereiding van dit verslag vragen voorgelegd over specifieke gegevensbeschermingsprincipes waaraan Europol zich moet houden. Malta werd gevraagd kenbaar te maken in welke mate overeenkomstig dezelfde principes te werk wordt gegaan. In dit hoofdstuk worden de antwoorden weergegeven.

3.1. Rechtmatigheid verwerking

Gegevens kunnen alleen overeenkomstig specifieke voorschriften worden verwerkt.

Hoewel dit principe niet is opgenomen in de wet inzake gegevensbescherming van 2001 noch in de regeling inzake gegevensbescherming, wordt met beide rechtsmiddelen bindende criteria vastgelegd voor gevallen waarin verwerking van persoonsgegevens kan plaatsvinden. Bijvoorbeeld, artikel 7 (a) en (c) van de wet inzake gegevensbescherming bepaalt dat de voor verwerking verantwoordelijke dient ervoor te zorgen dat:

- persoonsgegevens eerlijk en rechtmatig worden verwerkt;
- persoonsgegevens uitsluitend worden vergaard voor specifieke, expliciet opgegeven en rechtmatige doeleinden.

Artikel 9 van de wet inzake gegevensbescherming dient eveneens te worden vermeld, aangezien in dit artikel is vastgelegd in welke gevallen gegevens rechtmatig kunnen worden verwerkt. Aangezien deze rechtsmiddelen expliciet de rechtmatige gegevensverwerking regelen, is het duidelijk dat gegevensverwerking die hieronder niet ressorteert, verboden is.

3.2. Doel verwerking

Gegevens mogen alleen worden verwerkt voor duidelijk omschreven doeleinden

Dit principe is opgenomen in artikel 5, lid 1, van de regeling inzake gegevensbescherming dat als volgt luidt: de vergaring van persoonsgegevens voor politieke doeleinden dient in verhouding te staan tot de noodzaak voor preventie, bestrijding, onderzoek, opsporing en vervolging van specifieke misdrijven of voor de preventie van reëel gevaar, of zoals gestipuleerd in iedere andere wet. Dit principe wordt versterkt met artikel 6, lid 2, van de regeling inzake gegevensbescherming dat als volgt luidt: (2) voor politieke doeleinden vergaarde gegevens mogen niet worden verwerkt voor andere doeleinden die niet verenigbaar zijn met dergelijke politieke doeleinden.

3.3. Doel verstrekking

Gegevens mogen alleen aan derden worden verstrekt voor duidelijk omschreven doeleinden

Artikel 8 van de regeling inzake gegevensbescherming voorziet in een expliciete bepaling hieromtrent. Het artikel luidt als volgt: de gegevensuitwisseling tussen verscheidene politieke instanties is uitsluitend toegestaan indien er een rechtmatig belang bestaat voor dergelijke uitwisseling binnen het kader van de rechtsbevoegdheid van dergelijke instanties. Hierna volgt in voornoemd artikel een overzicht van de andere specifieke gevallen waarin gegevens mogen worden verstrekt aan overheidsinstanties of particulieren.

Het artikel besluit in lid 4 dat gegevens uitsluitend mogen worden verstrekt indien de gegevens noodzakelijk zijn voor de ontvanger om zijn rechtmatige taak te voltooien en mits het doel voor de door de ontvanger uit te voeren verwerking verenigbaar is met de oorspronkelijke verwerking of niet strijdig is met de wettelijke verplichtingen van de politieke instanties. Bovendien regelt artikel 10 van de regeling inzake gegevensbescherming bijzonderheden over de manier van verwerking van verzoeken om gegevensverstrekking. In deze regeling is opgenomen dat de verzoekende partij het doel moet aangeven waarvoor zij de gegevens nodig heeft, alsook het principe dat de gegevens uitsluitend mogen worden gebruikt voor de doelen waarvoor ze werden aangevraagd.

3.4. Kwaliteit gegevens

Verwerkte gegevens moeten accuraat zijn en, zo nodig, bijgewerkt worden

Twee verwijzingen naar dit principe zijn opgenomen in artikel 6 van de regeling inzake gegevensbescherming. De eerste is terug te vinden in het eerste lid en luidt als volgt: de verwerking van persoonsgegevens voor politieke doeleinden moet, indien mogelijk, beperkt blijven tot nauwkeurige gegevens (...). De tweede verwijzing is opgenomen in het vierde lid en luidt als volgt: “De voor verwerking verantwoordelijke moet redelijke maatregelen nemen om gegevens aan te vullen, te wijzigen, blokkeren of schrappen indien deze onvolledig of onjuist zijn voor de politieke doeleinden waarvoor ze worden verwerkt.” Bovendien wordt in artikel 11 het volgende gesteld: bij gegevensverstrekking dienen de volgende regels, voorzover mogelijk, in acht te worden genomen: (a) de nauwkeurigheid van de gegevens moet worden gecontroleerd vóór de eerste openbaarmaking hiervan.” In het vierde lid van artikel 11 wordt tevens het volgende bepaald: “(d) gegevens die niet langer nauwkeurig of actueel zijn, mogen niet worden verstrekt. Indien wordt vastgesteld dat gegevens die werden verstrekt niet nauwkeurig of actueel zijn, moet de ontvanger op de hoogte worden gebracht tenzij het verstrekken van dergelijke informatie onevenredig veel moeite zou kosten.”

3.5. Evenredigheid

Gegevens moeten toereikend, ter zake dienend en niet excessief zijn ten opzichte van de doeleinden waarvoor ze worden verzameld, overgedragen of verder verwerkt.

Dit principe is eveneens vastgelegd in artikel 6, lid 1, van de regeling inzake gegevensbescherming. Hierin lid wordt bepaald dat de verwerking van persoonsgegevens voor politieke doeleinden indien mogelijk moet worden beperkt tot nauwkeurige en noodzakelijke gegevens zodat de instantie met openbaar gezag haar functie kan uitvoeren overeenkomstig de wet en internationale verplichtingen kan nakomen die voortvloeien uit een conventie, verdrag of bilaterale overeenkomst met betrekking tot politieke aangelegenheden waarvan Malta deel uitmaakt. In deze context kan tevens worden verwezen naar artikel 5, lid 1, dat reeds werd aangehaald onder punt 3.2., en waarin wordt bepaald dat uitsluitend gegevens voor politieke doeleinden mogen worden vergaard.

3.6. Termijnen

Gegevens kunnen uitsluitend voor een vastgestelde periode worden opgeslagen en moeten regelmatig gecontroleerd worden om na te gaan of ze nog steeds ter zake dienend zijn.

Artikel 6, lid 2, van de regeling inzake gegevensbescherming bepaalt dat “Voor politieke doeleinden verwerkte persoonsgegevens niet langer dan noodzakelijk mogen worden opgeslagen gelet op de politieke doeleinden waarvoor we worden verwerkt.” Er bestaat echter geen specifieke verplichting de gegevens regelmatig op relevantie voor dergelijke doeleinden te controleren. Hoewel een dergelijke controle ogenschijnlijk de enige manier is om de tenuitvoerlegging van het algemene beginsel van artikel 6, lid 2, te waarborgen, is dit niet wettelijk geregeld. De Maltese instanties overwegen de bewaarperiodes en herzieningsprocedures te ontwikkelen en goed te keuren. Derhalve lijkt het nodig deze kwestie afzonderlijk in een internationale overeenkomst te regelen.

3.7. Overdracht van gegevens aan derden

Gegevens mogen alleen aan derden worden overgedragen indien aan specifieke voorwaarden wordt voldaan. Een dergelijke overdracht moet naar behoren worden geregistreerd en alle door de gegevensverstrekker opgelegde beperkingen dienen te worden gerespecteerd.

Zoals reeds vermeld onder punt 3.3., voorziet de regeling inzake gegevensbescherming expliciet in een regeling van gevallen waarin persoonsgegevens kunnen worden verstrekt aan derde partijen, alsook de te volgen procedure met betrekking tot dergelijke verzoeken. Dit principe is opgenomen in artikelen 8 en 10 van de regeling inzake gegevensbescherming. De verplichting om gegevensverstrekkingen te registreren is vervat in het derde lid van artikel 10: “De politieke instantie moet een register bijhouden van alle verstrekte persoonsgegevens met vermelding van: (a) de details van de verzoekende instantie; (b) het doel en de reden van het verzoek; (c) de datum van de gegevensverstrekking.”

Bovendien regelt artikel 9 van de regeling inzake gegevensbescherming de gegevensverstrekking aan derde landen. In dit artikel worden de ontvangers beperkt tot politieke instanties en wordt bovendien bepaald in welke gevallen dergelijke verstrekkingen zijn toegestaan. Deze voorschriften zijn gebaseerd op principe 5.5. van aanbeveling R (87) 15.

Niettegenstaande wordt de ontvangende partij, zoals in de meeste andere gevallen, daarin niet met zoveel woorden verplicht de door de gegevensverstrekker opgelegde beperkingen te respecteren. Derhalve dient de plicht om de beperkingen in verband met de verwerking van door Europol verstrekte persoonsgegevens te respecteren, deel uit te maken van een overeenkomst tussen Europol en Malta.

3.8. Gevoelige gegevens

Gevoelige gegevens zoals vermeld in het eerste lid van artikel 6 van het Verdrag van de Raad van Europa inzake gegevensbescherming vereisen speciale beschermende maatregelen.

Het vraagstuk van de verwerking van gevoelige gegevens is vastgelegd in artikel 5, lid 4, van de regeling inzake gegevensbescherming waarin wordt gesteld dat: de verwerking van gevoelige persoonsgegevens is toegestaan indien dit noodzakelijk is in het kader van een bijzonder onderzoek. Hieromtrent zijn geen verdere bepalingen opgenomen in de regeling inzake gegevensbescherming en zoals reeds aangehaald zijn de in de wet inzake gegevensbescherming opgenomen voorschriften met betrekking hiertoe, niet van toepassing.

Aangezien dit niet volledig strookt met de geldende regels van Europol, is het wenselijk een expliciete bepaling op te nemen in de overeenkomst tussen Europol en Malta voor gevallen waarin gevoelige persoonsgegevens kunnen worden uitgewisseld, overeenkomstig het algemeen juridisch kader van Europol.

3.9. Beveiliging van de gegevens

Er moeten technische en organisatorische maatregelen worden genomen om de volledigheid van de verwerkte gegevens te waarborgen

Een algemene bepaling met betrekking tot gegevensbeveiliging is vastgelegd in artikel 14 van de regeling inzake gegevensbescherming dat als volgt luidt: de voor verwerking verantwoordelijke moet juiste technische en organisatorische maatregelen ten uitvoer leggen om de bescherming van persoonsgegevens te waarborgen tegen accidentele of onrechtmatige vernietiging of verlies of iedere vorm van onrechtmatige verwerking en moet hierbij een toereikend beveiligingsniveau waarborgen met inachtneming van:

- (a) de beschikbare technische mogelijkheden;
- (b) de kosten van de tenuitvoerlegging van beveiligingsmaatregelen;
- (c) de bijzondere risico's inzake de verwerking van persoonsgegevens;
- (d) de gevoeligheid van de te verwerken persoonsgegevens.

Het tweede lid stelt bovendien dat indien de voor verwerking verantwoordelijke gebruik maakt van een verwerker, de voor verwerking verantwoordelijke zich ervan moet vergewissen dat de verwerker dergelijke, door de voor verwerking verantwoordelijke opgelegde beveiligingsmaatregelen kan en moet ten uitvoerleggen.

3.10. Het opstellen van rapporten

Er moeten technische en organisatorische maatregelen zijn teneinde te verifiëren dat toegang tot gegevens is verkregen overeenkomstig de ter zake dienende voorschriften

Noch in de wet inzake gegevensbescherming, noch in de regeling inzake gegevensbescherming zijn specifieke bepalingen opgenomen met betrekking tot het opstellen van rapporten over toegang tot door politieke instanties verwerkte persoonsgegevens. De Maltese autoriteiten hebben echter Europol op de hoogte gebracht dat:

- Er binnen de politiediensten interne toegangsprocedures bestaan;
- een controlespoor wordt bijhouden van alle gebruikers die toegang krijgen tot de politiestructuren;

- gecentraliseerde procedures eventuele “bewegingen” van bestanden registreren;
- Government’s Central Information Management Unit (gecentraliseerde overheidsdienst voor informatiebeheer) (CIMU) een gestandaardiseerd beleid voor informatiebeveiliging aan het voorbereiden is (zie www.cimu.gov.mt) voor de overheidsdiensten, inclusief de politie overeenkomstig BS 7799.
- De politie stelt tevens alles in het werk om de in het CIMU-handboek gepubliceerde richtsnoeren ter bestrijding van computermisbruik te volgen, met name om de instanties te verwittigen over onrechtmatige toegang en gebruik van informatie.

3.11. Doorzichtigheid

De betrokkene heeft het recht om (op verzoek) geïnformeerd te worden over op hem betrekking hebbende verwerkte gegevens en om, indien er geen redenen zijn om de gegevens achter te houden, correctie of verwijdering van dergelijke gegevens te verkrijgen

De rechten van betrokkenen wat betreft toegang tot en correctie en verwijdering van eigen persoonsgegevens zijn nauwkeurig beschreven in artikel 13 van de regeling inzake gegevensbescherming. Dit artikel bevat alle gebruikelijke bepalingen betreffende de rechten van de betrokkene inzake toegang tot, correctie, blokkering of verwijdering van gegevens (lid 1), de te volgen procedure (lid 2), de reden waarom een verzoek kan worden geweigerd (lid 3), de verplichting een met redenen omkleed besluit te nemen inzake de verzoeken en het verzoek in te willigen indien geen reden bestaat voor weigering (lid 4), alsook het recht om beroep aan te tekenen tegen het besluit bij de functionaris voor gegevensverwerking (leden 5 en 6).

3.12. Aansprakelijkheid

De betrokkene heeft het recht op vergoeding voor geleden schade als gevolg van de onjuiste verwerking van gegevens

Artikel 46 van de wet inzake gegevensbescherming luidt als volgt: “De betrokkene kan bij dagvaarding een beroep voor geleden schade instellen bij de bevoegde rechtbank tegen de voor verwerking verantwoordelijke die de gegevens heeft verwerkt die gehandeld heeft in strijd met de respectieve wet of regeling.” Gezien de verwijzingen naar de regelgeving in deze wet, is dit artikel tevens van toepassing indien dit geschiedt in het kader van de verwerking van persoonsgegevens door politieke instanties.

3.13. Toezichthoudende autoriteit

Naleving van beginselen betreffende gegevensbescherming wordt gewaarborgd en toezicht hierop wordt uitgeoefend door een onafhankelijke toezichthoudende autoriteit

Het nationaal toezichthoudend orgaan is de functionaris voor gegevensbescherming. De artikelen van de wet inzake gegevensbescherming die betrekking hebben op het bureau van de functionaris voor gegevensbescherming (artikelen 36 tot 53) zijn later in werking getreden dan de wet zelf, met name op 22 maart 2002 (wettelijke kennisgeving nr. 70 van 2002). Bijgevolg werd de functionaris voor gegevensbescherming benoemd op 26 maart 2002. Artikelen 36 tot en met 53 regelen de gebruikelijke aangelegenheden over de op de oprichting van een onafhankelijk toezichthoudend orgaan, inclusief de toelatingsvereisten voor dit Bureau, de nauwkeurige taken, functies en bevoegdheden van de functionaris, zijn taak met betrekking tot voor verwerking verantwoordelijken enz. Over het algemeen omvatten zijn taken:

- “(a) het aanleggen en onderhouden van een openbaar register van alle verwerkingsoperaties overeenkomstig de hem toegewezen informatie, zoals vastgelegd in deze wet;
- (b) het uitoefenen van toezicht en het nagaan, op eigen initiatief of op verzoek van de betrokkene, of de verwerking is uitgevoerd overeenkomstig de bepalingen van de respectieve wet of regeling;
- (c) het instrueren van de verwerker en de voor verwerking verantwoordelijke om maatregelen te nemen teneinde te kunnen waarborgen dat de verwerking wordt uitgevoerd overeenkomstig de respectieve wet en regeling;
- (d) het ontvangen van rapporten en vorderingen van betrokkenen of verenigingen die hem vertegenwoordigen met betrekking tot schendingen van de respectieve wet en regeling, het zoeken naar oplossingen voorzover dit voor hem noodzakelijk lijkt of door de wet verplicht is en het op de hoogte brengen van de betrokkenen of verenigingen van de resultaten;
- (e) het opstellen van richtsnoeren voorzover dit van hem wordt verwacht voor de doelstellingen van deze wet;
- (f) het instellen van gerechtelijke procedures in burgerzaken in gevallen waarin de bepalingen van deze wet worden of werden geschonden en het verwijzen van ieder, in of bij de uitoefening van zijn taken voorgedaan misdrijf naar de openbare, bevoegde instanties;
- (g) het aanmoedigen van het opstellen van geschikte gedragscodes door de verscheidene sectoren die betrokken zijn bij de bepalingen van deze wet en het vaststellen dat de bepalingen van dergelijke codes in overeenstemming zijn met de bepalingen van de wet en derhalve kan de functionaris de betrokkene of hun vertegenwoordigers verzoeken hun mening te uiten;

(h) het nemen van maatregelen om het groot publiek op de hoogte te brengen van de bepalingen van de wet en bijgevolg, indien nodig, het geven van advies aan individuen;

(i) opdracht geven tot blokkering, verwijdering of vernietiging van gegevens, het tijdelijk of definitief verbieden van verwerking of het waarschuwen of berispen van de voor verwerking verantwoordelijke;

(j) het adviseren van de overheid in verband met eventuele wettelijke maatregelen die vereist zijn teneinde zijn functie naar behoren te kunnen uitoefenen;

(k) het op gezette tijden (tenminste jaarlijkse) opstellen van jaarlijkse rapporten over zijn werkzaamheden op regelmatig. De rapporten moeten openbaar worden gemaakt;

(l) het op verzoek van de betrokkene nagaan of de in artikel 23 van de wet beschreven verwerking van persoonsgegevens verenigbaar is met de bepalingen van de wet of iedere andere wet, zoals vastgelegd in sub-artikel (1) van genoemd artikel 23 en in voorkomend geval moet de betrokkene hiervan op de hoogte worden gebracht;

(m) het samenwerken met de toezichthoudende organen of met andere landen voorzover noodzakelijk voor de uitoefening van zijn functie, met name door de uitwisseling van alle nuttige informatie in overeenstemming met iedere conventie waarvan Malta deel uitmaakt of met iedere internationale verplichting van Malta.” (artikel 40 van de wet inzake gegevensbescherming).

Hoewel de wet inzake gegevensbescherming van 2001 niet van toepassing is op de verwerking van persoonsgegevens door politieke instanties (artikel 5 van de wet), verwijst de functiebeschrijving van de functionaris naar voorschriften die hierop zijn gebaseerd, waaronder de regeling inzake gegevensbescherming. De regeling inzake gegevensbescherming regelt tevens bepaalde bevoegdheden van de functionaris, zoals de verplichting van de voor verwerking verantwoordelijken om hun verwerkingsoperaties te registreren (artikel 4) en de bevoegdheid om te beslissen over beroepen met betrekking tot verzoeken om toegang, correctie of vernietiging. Dit betekent dat de functionaris voor gegevensbescherming volledig verantwoordelijk is voor zijn taken en bevoegdheden, ook met betrekking tot de verwerking van persoonsgegevens door politieke instanties.

4. BESTUURSRECHTELIJKE PRAKTIJK

De Maltese ratificatie van het Europese Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden en van de aanvullende protocollen houdt in dat deze instrumenten deel zijn gaan uitmaken van de eigen wetgeving, en dat zij voorrang genieten boven elk ander nationaal rechtsmiddel.

Elke burger die van mening is dat zijn/haar rechten zijn geschaad, heeft het recht de openbare instanties hierop direct aan te spreken, ofwel via administratieve kanalen, dan wel via de ombudsman, of zich te wenden tot de daartoe bevoegde rechtbanken, waaronder het Europese Hof voor de rechten van de mens.

Wat betreft de eigenlijke bescherming van gegevens is duidelijk dat de bestuursrechtelijke praktijk op dit gebied zich nog in de eerste fase van zijn ontwikkeling bevindt. Dit is niet verwonderlijk aangezien het feit dat de nieuwe wet inzake gegevensbescherming slechts in werking trad op 14 december 2002. Derhalve is het thans te vroeg meer nauwkeurigheden te verstrekken over de manier van tenuitvoerlegging van de nieuwe wet en regelgevingen. Naar verwachting moet echter vooruitgang worden geboekt op het ogenblik dat een overeenkomst tussen Europol en Malta in werking zal treden. Momenteel kan melding worden gemaakt van het feit dat zogenaamde verantwoordelijken voor gegevensbescherming zijn tewerkgesteld bij overheidsdiensten en bij de politiesector. Voorlichtingsbijeenkomsten over gegevensbescherming voor de politie werden eveneens georganiseerd. In het kader van de bilaterale overeenkomst wordt eveneens een specifiek project met betrekking tot gegevensbescherming opgezet.

5. CONCLUSIE

Op basis van het onderhavige verslag komt de raad van bestuur tot de conclusie dat de wetgeving op het gebied van gegevensbescherming en de bestuursrechtelijke praktijk in Malta van dien aard is dat hij de Raad adviseert te besluiten dat met onderhandelingen over de verstrekking van persoonsgegevens door Europol kan worden aangevangen.

Er zijn slechts enkele bijzonderheden waarop de raad van bestuur de aandacht van de Raad wenst te vestigen.

Ten eerste schijnen er op het niveau van algemene wetgeving geen duidelijke bewaartermijnen te zijn vastgelegd voor persoonsgegevens. Evenmin is op dit niveau voorzien in periodieke herzieningen. Om die reden is het aanbevolen desbetreffende bepalingen toe te voegen aan de te ondertekenen overeenkomst.

Ten tweede dient te worden opgemerkt dat het wettelijke kader niet met zoveel woorden bepaalt dat de door de verstrekker van de gegevens opgelegde beperkingen moeten worden gerespecteerd. Gezien het ontbreken van dergelijke bepalingen dient de plicht om de beperkingen in verband met de verwerking van door Europol verstrekte persoonsgegevens te respecteren, deel uit te maken van een overeenkomst tussen Europol en Malta.

Ten derde zij de aandacht gewezen op het ontbreken van nauwkeurige bepalingen inzake de verwerking van gevoelige gegevens. Zoals reeds onder punt 3.8 is aangegeven, dient de uitwisseling van gevoelige gegevens eveneens in de overeenkomst te worden geregeld, en wel volgens het voorbeeld van het huidige wettelijk kader van Europol op dit gebied.

**HET GEMEENSCHAPPELIJK CONTROLEORGAAN
VAN EUROPOL**

**Advies van het GCO in verband met
het niveau van de gegevensbescherming in Malta**

Ter attentie van:

*de voorzitter van de
raad van bestuur van Europol
dhr. N. Tasiopoulos
Postbus 90850
NL-2509 LW Den Haag*

DOCUMENT 03/20

HET GEMEENSCHAPPELIJK CONTROLEORGAAN VAN EUROPOL,

A. Inleidende opmerkingen

1. Het GCO is verzocht een advies op te stellen inzake de wetgeving en bestuursrechtelijke praktijken van Malta op het gebied van gegevensbescherming op basis van het door Europol voorgelegde verslag (met dossiernr. 2641-36).
2. Dit verslag is door de raad van bestuur van Europol voorgelegd aan het GCO overeenkomstig artikel 1, lid 5, van het besluit van de Raad waarbij de directeur van Europol wordt gemachtigd om onderhandelingen te openen met derde landen en niet aan de EU verwante instellingen met het oog op te sluiten overeenkomsten.
3. In artikel 3, lid 3, tweede deel, van de regels betreffende de verstrekking van persoonsgegevens aan derde landen en instanties wordt expliciet erkend dat het GCO eveneens advies dient uit te brengen tijdens de procedure waarin de Raad van de Europese Unie moet besluiten al dan niet zijn goedkeuring te hechten aan overeenkomsten tussen Europol en Malta. Het GCO onderstreept derhalve dat het onderhavige advies alleen betrekking heeft op de vraag of er voor Europol belemmeringen bestaan om onderhandelingen te starten met Malta die eventueel kunnen leiden tot een overeenkomst over de verstrekking van persoonsgegevens door Europol aan Malta. Dit advies bindt het GCO geenszins bij het opstellen van zijn advies met betrekking tot de uiteindelijke overeenkomst tussen Europol en Malta.

4. Niettegenstaande het voorgaande punt benadrukt het GCO echter dat de kwesties die in het onderhavige advies te berde worden gebracht, in de met Malta te onderhandelen overeenkomst aan de orde gesteld dienen te worden. Bij zijn advies inzake de overeenkomst als dusdanig zal het GCO er zeker rekening mee houden of het uiteindelijke voorstel voor een overeenkomst toereikende oplossingen bevat voor de hierna genoemde kwesties.
5. Het GCO vestigt de aandacht op het feit dat het onderhavig advies uitsluitend is gebaseerd op het verslag vervat in dossier nr. 2641-36 van 20 maart 2003. Dit houdt in dat het GCO zijn advies baseert op de feiten zoals die in dat verslag naar voren zijn gebracht. Een verandering in het niveau van gegevensbescherming door Malta zou zonder enige twijfel van invloed zijn op het advies van het GCO met betrekking tot de overeenkomst.

B. Advies van het GCO inzake Malta

Het GCO is van oordeel dat er, gezien de feiten en conclusies die in dossier nr. 2641-36 naar voren zijn gebracht, vanuit het gezichtspunt van gegevensbescherming voor Europol geen belemmeringen bestaan om onderhandelingen te starten met Malta als voorbereiding op een overeenkomst met betrekking tot de verstrekking van persoonsgegevens door Europol aan Malta.

Bij het opstellen van zijn advies heeft het GCO rekening gehouden met de Maltese wetgeving op het gebied van gegevensbescherming, met inbegrip van het bestaan van de functionaris voor gegevensbescherming, zoals vastgelegd in het verslag. Het GCO benadrukt het feit dat Europol de relevante wetten en regelgevingen niet heeft ingediend en dat bijgevolg het huidige advies uitsluitend is gebaseerd op het hierboven genoemde verslag.

Het GCO merkt uitdrukkelijk op dat aangezien de Maltese wetgeving op het gebied van gegevensbescherming niet van toepassing is op gegevensverwerking door diensten van politie en justitie, er nog geen ervaring is met de bestuursrechtelijke praktijken op het gebied van gegevensbescherming en rechtshandhaving. Regeling inzake gegevensbescherming 2002 die de verwerking van persoonsgegevens in de politiesector regelt, is nog niet in werking getreden. Het GCO benadrukt dat de overdracht van gegevens van Europol aan Malta niet dient plaats te vinden vóór de inwerkingtreding van deze regeling.

Het GCO benadrukt de noodzaak om het GCO in kennis te stellen van de ontwikkelingen betreffende de Maltese wetgeving aangezien het GCO zal worden verzocht zijn advies over de ontwerp-overeenkomst uit te brengen.

C. Bij onderhandelingen met Malta in acht te nemen punten

- a) In de overeenkomst dient te worden vastgelegd dat verstrekking van persoonsgegevens aan Malta alleen kan plaatsvinden wanneer het doel en de reden voor de overdracht voldoende duidelijk is aangegeven, en wanneer de overdracht valt binnen (a) de reikwijdte van de Europol-overeenkomst en (b) de reikwijdte van de overeenkomst tussen Europol en Malta. Verder moeten er garanties bestaan dat Malta de door Europol verstrekte gegevens alleen kan aanwenden voor de in de overeenkomst vastgelegde doelen, die natuurlijk overeen dienen te komen met de doelen zoals vastgelegd in de Europol-overeenkomst. Het GCO beveelt aan in de overeenkomst een bepaling op te nemen die waarborgt dat de door Europol verstrekte gegevens alleen overeenkomstig de bepalingen van de overeenkomst zullen worden verstrekt.

Men dient zich volledig te houden aan artikel 6, lid 1, eerste deel alsook artikel 6, lid 2 van de regels betreffende de verstrekking van persoonsgegevens door Europol aan derde landen en instanties.

- b) In de overeenkomst dient ook te worden vastgelegd dat Malta de plicht heeft alle van Europol ontvangen gegevens te vernietigen zodra zij niet langer van belang zijn voor het doel waarvoor zij zijn verstrekt (zie artikel 7, lid 3 van de regels betreffende de verstrekking van persoonsgegevens).
- c) De tijdslimieten voor de opslag van persoonsgegevens zoals vastgelegd in de Europol-overeenkomst en de bijbehorende tenuitvoerleggingregels dienen van toepassing te worden gemaakt op de door Europol aan Malta verstrekte gegevens teneinde zeker te stellen dat Malta gegevens niet langer opslaat dan aan Europol toegestaan zou zijn. Het GCO beveelt aan in de overeenkomst een bepaling op te nemen die waarborgt dat gegevens alleen mogen worden opgeslagen voor een duidelijk bepaalde periode en dat de relevantie van de gegevens regelmatig moet worden gecontroleerd.
- d) Verdere overdracht door Malta van door Europol verstrekte persoonsgegevens aan derde landen dient te worden uitgesloten bij afwezigheid van specifieke uitzonderingen waarbij artikel 5, lid 5, van het besluit van de Raad betreffende de verstrekking van persoonsgegevens aan derde landen en instanties van toepassing is.

- e) Een directe verbinding tussen de computersystemen van Europol en Malta zou een inbreuk op de Europol-overeenkomst betekenen. Derhalve verzoekt het GCO dat ervoor wordt gezorgd dat bij verstrekking van persoonsgegevens door Europol aan Malta een procedure wordt gevolgd die een toereikend niveau van gegevensbescherming waarborgt. Bovendien dienen voldoende veiligheden te worden ingebouwd bij de opslag en het gebruik van gegevens door Malta.
- f) De overeenkomst dient specifieke bepalingen betreffende de verwerking van gevoelige gegevens te bevatten. Deze bepalingen moeten garanderen dat de verplichtingen van Europol worden gerespecteerd.
De bepalingen in de regeling inzake gegevensbescherming 2002 wijken op dit gebied af van de geldende regels van Europol. De in hoofdstuk 3.8 van het verslag vermelde suggestie dient te worden gevolgd.
- g) In de overeenkomst dient te worden benadrukt dat de verstrekking van gevoelige gegevens door Europol aan Malta slechts plaats kan vinden als Malta voor elk geval een duidelijke, met redenen omklede behoefte aan de te verstrekken gegevens aantoont. Artikel 6, lid 1, tweede deel, van de regels betreffende de verstrekking van persoonsgegevens aan derde landen en instanties dient in dit verband nauwgezet nageleefd te worden.
- h) Overeenkomstig artikel 7 van de regels betreffende de verstrekking van persoonsgegevens door Europol aan derde landen en instanties dient Europol Malta onmiddellijk in kennis te stellen van alle wijzigingen in de gegevens die door Europol aan Malta zijn verstrekt. In de overeenkomst dient te worden vastgelegd dat Malta, zodra het een dergelijke kennisgeving ontvangt, verplicht is de betreffende gegevens via wijziging of verwijdering in overeenstemming te brengen met de nieuwe van Europol ontvangen informatie.
- i) Het principe om verslagen op te stellen over opvragingen dient te worden opgenomen in de overeenkomst.
- j) Er dient voldoende toezicht gehouden te worden op de toepassing van de overeenkomst, en men dient erin te voorzien dat Malta tegenover individuele personen aansprakelijk is voor inbreuk op de overeenkomst en voor niet-geautoriseerde of onjuiste verwerking van gegevens (zie artikel 8 van de regels betreffende de verstrekking van persoonsgegevens aan derde landen en instanties).

- k) Voor Malta dient te worden benadrukt dat het door dit land geboden veiligheidsniveau voor door Europol overgedragen persoonsgegevens beoordeeld dient te worden met inachtneming van het in artikel 25 van de Europol-overeenkomst vastgestelde kader.
- l) Het beginsel van het aanvaarden van voorwaarden naargelang het gebruik van de gegevens dient te worden opgenomen in de overeenkomst. De in hoofdstuk 3,7 van het verslag vermelde suggestie dient te worden gevolgd.
- m) Overwegende dat de regeling inzake gegevensbescherming 2002 nog niet in werking is getreden, is de overdracht van gegevens van Europol aan Malta niet mogelijk vóór de inwerkingtreding hiervan.

D. Slotopmerkingen

Zoals reeds aangehaald, verzoekt het GCO Europol ook in de toekomst voorzien te worden van alle relevante informatie om op de hoogte te kunnen blijven van alle relevante ontwikkelingen wat Malta betreft. Het GCO zou het op prijs stellen als het in de toekomst op passende wijze betrokken zou blijven bij het proces dat moet leiden tot het sluiten van een overeenkomst met Malta. In dit verband is het GCO bereid Europol alle bijstand te bieden die nodig is.

*Brussel,
7 mei 2003*

*Klaus KALK
Voorzitter van het
gemeenschappelijk controleorgaan
van Europol*