Federale Overheidsdienst Binnenlandse Zaken
Algemene Directie Instellingen en Bevolking
Rijksregister

Nota aan de Gebruikers van het Rijksregister

Uw contactpersoon	**T**	**Uw referentie**	**Bijlagen**
C.Rouma	02 518 20 31		1
E-mail	**F**	**Onze referentie**	**Brussel**
christiane.rouma@ibz.fgov.be	02 518 21 25	III/30/1794/08	12 maart 2008

Bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.- Toegang tot de informatiegegvens van het Rijksregsiter.-Veiligheidsmaatregelen die ertoe strekken de vertrouwelijkheid en de integriteit van de gegevens, de authentificatie van de gebruikers en het spoor van activiteiten die uitgevoerd werden op de informatiesystemen, te waarborgen

Geachte dames en heren,

In mijn omzendbrief aan de gebruikers van 24 september 2007 (refertenummer:III30/5650/07), die hier als bijlage gevoegd wordt, heb ik hun aandacht gevestigd op de verplichting voor alle overheden en instellingen die, met het oog op bijwerking en/of raadpleging, gemachtigd zijn om toegang te hebben tot het bestand van de natuurlijke personen, om technische en organisatorische maatregelen te implementeren die van dien aard zijn dat zij, gelet op de vooruitgang van de techniek, de veiligheid, de integriteit, de vertrouwelijkheid en de juistheid van de gegevens kunnen waarborgen.

Tijdens de bijeenkomst van de leden van het Sectoraal Comité van het Rijksregister en van de vertegenwoordigers van de Algemene Directie Instellingen en Bevolking, die plaatsvond op 13 februari jl., werden bepaalde belangrijke punten met betrekking tot de bepaling van de veiligheidsmaatregelen die de beveiliging van de informatiegegevens van het Rijksregister tijdens hun verwerking moeten waarborgen, in het bijzonder behandeld.

Het lijkt me noodzakelijk u op de hoogte te brengen van de punten die speciale aandacht genoten hebben en die, ten einde risico's op de schending van de persoonlijke levenssfeer te vermijden, eventueel op technisch en organisatorisch vlak de invoering van nieuwe schikkingen vereisen.

1.Logische beveiliging van de toegangen:

De personen die gemachtigd zijn om toegang te hebben tot de informatiegegevens van het Rijksregister en om ze te verwerken moeten duidelijk geïdentificeerd zijn, alsmede hun respectievelijke machtigingen. De personenlijst moet bijgehouden en geactualiseerd worden.

De uitgebreidheid van de machtigingen moet strikt gepreciseerd zijn en deze machtigingen moeten aangeduid worden door technische maatregelen voor de controle op de toegang niet alleen tot de gegevens zelf maar eveneens tot de informaticabestanddelen (programma's, telecommunicatie-uitrustingen, drager voor het opslaan). De identificatie van de interveniënten zal aangevuld worden door een authentificatieprocedure die het mogelijk maakt de volledige opvolging te verwezenlijken van de procedure tot bescherming van de persoonlijke levenssfeer. Een systeem van intern beheer van de toegangen tot de verschillende toepassingen en functionaliteiten van het informaticasysteem, gecombineerd met het archiveren van alle uitgevoerde interventies, maakt het mogelijk om deze doelstelling te bereiken.

In deze optiek zal binnenkort een intern centraal systeem voor het beheer van de toegangen tot de "IAM"-toepassingen binnen het Rijksregister verwezenlijkt worden; dit systeem zal berusten op de authentificatie van de personeelsleden, die toegang hebben tot de genoemde toepassingen, door middel van de elektronische identiteitskaarten.

Het zou nuttig zijn dat organisatorische maatregelen de technische maatregelen voor de controle en de toegang, door sommige personeelsleden, tot bepaalde kritieke toepassingen, zoals bijvoorbeeld het systeem voor het beheer van de gebruikers of de programma's voor het verwerken van archiefbestanden, komen aanvullen. Vergissingen, oneigenlijk gebruik en kwaadwillige daden die op dit vlak bedreven worden, kunnen ernstige gevolgen hebben op het vlak van de bescherming van de persoonlijke levenssfeer (machtiging tot toegang die niet mocht verleend worden aan bepaalde personen, het uitwissen of het nalaten van sporen van de uitgevoerde verrichtingen). In deze context dient het werk zó georganiseerd te worden dat deze verrichtingen niet uitgevoerd worden door een geïsoleerde operateur.

2.Mededeling van de informatiegegevens van het Rijksregister onder de vorm van uittreksels.

De mededeling van de informatiegegevens van het Rijksregister (onder de vorm van uittreksels) aan de overheden en instellingen bedoeld in artikel 5 van de wet van 8 augustus 1983 tot regeling van een Rijksregister wordt onder bepaalde voorwaarden toegestaan door het Sectoraal Comité. Deze machtiging wordt verleend in het kader van bepaalde doeleinden.

De voorwaarden onder de welke de gegevens kunnen gebruikt worden en de duur gedurende de welke zij kunnen bewaard worden, worden eveneens nader bepaald in de beraadslaging van het Sectoraal Comité.

De veiligheidsconsulent die aangewezen is door de verantwoordelijke overheden op het niveau van het organisme van de gebruikers, wordt in het bijzonder ermee belast de voornoemde voorwaarden te doen naleven.

Het Sectoraal Comité van het Rijksregister heeft ons gemeld dat sommige instellingen, die de machtiging ontvangen hebben om de mededeling te krijgen van bepaalde informatiegegevens, mits naleving van duidelijke voorwaarden aangaande de termijn voor het bewaren van de gegevens (beperkte termijn die inhoudt dat de gegevens uitgewist worden na het vervallen van de termijn) en aangaande het gebruik van deze gegevens (het is duidelijk bepaald: intern gebruik), de genoemde voorwaarden niet respecteren , hetzij dat zij de gegevens langer bewaren dan de vastgestelde termijnen, hetzij dat zij de gegevens mededelen aan derden, hetgeen in strijd is met hun verbintenis om deze gegevens slechts intern te gebruiken.

Park Atrium
Koloniënstraat 11 T 02 518 21 31 callcenter.rrn@rrn.fgov.be
1000 Brussel F 02 210 10 31 www.ibz.rrn.fgov.be

Hoef ik het te onderstrepen dat dergelijke praktijken onwettelijk zijn. De personen die dergelijke praktijken plegen, stellen zich bloot aan de strafbepalingen die vastgesteld zijn in artikel 13 van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen en in de artikelen 38 en 43 van de wet van 18 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

3. De technische en organisatorische beveiligingsmaatregelen moeten gecontroleerd worden op hun efficiëntie en moeten bijgewerkt worden in functie van de evolutie.

Er dient een bewakingssysteem verwezenlijkt te worden om zich ervan te vergewissen dat de veiligheidsmaatregelen die geïmplementeerd zijn om de verwerkte informatiegegevens te beveiligen, wel degelijk hun doel bereiken. Ten minste één keer per jaar dient er een heronderzoek van de genoemde maatregelen te geschieden om, zo nodig, correcties uit te voeren en aanpassingen aan te brengen.

Een audit dat door een extern organisme gerealiseerd wordt, zou in deze context, nuttig kunnen blijken.

4. Het belang van de communicatie (informatie en opleiding van het personeel).

De beveiliging van informaticasystemen is sterk afhankelijk van de juiste informatie die verstrekt wordt aan het personeel dat rechtstreeks of onrechtstreeks tussenkomt bij de verwerking van de informatiegegevens.

De voorzorgsmaatregelen en ieders verplichtingen en verantwoordelijkheden dienen uiteengezet te worden tijdens informatievergaderingen waarbij er zal moeten herinnerd worden aan de procedures die bepaald werden om de integriteit en de vertrouwelijkheid van de gegevens te verzekeren.

Wat deze procedures aangaat, dient men vooral te zorgen voor een streng beheer van de sleutels van het Rijksregister (variabele sleutels : login – paswoord of vaste sleutels), in het bijzonder wat de identificatie van de titularissen van de sleutels (wat de veranderlijke sleutels aangaat) en wat het bijhouden van de desbetreffende informatiegegevens betreft. Zo ook dient de aandacht van de titularissen van de sleutels gevestigd te worden op de verplichting de vertrouwelijkheid van de genoemde sleutels te bewaren (het is verboden de logins en de sleutels op een papieren drager over te schrijven en ze zichtbaar te laten voor derden).

Als gebruikers van het Rijksregister, bent u onze partners voor het bereiken van de doelstelling om voortdurend de veiligheid van de informatiegegevens van het Rijksregister te verbeteren ten einde het hoogstmogelijke niveau van beveiliging te verzekeren tegen schendingen van de privacy in het kader van de verwerking van deze gegevens.

Hoogachtend,

L.VANNESTE.

Directeur-generaal.

Park Atrium
Koloniënstraat 11 T 02 518 21 31 callcenter.rrn@rrn.fgov.be
1000 Brussel F 02 210 10 31 www.ibz.rrn.fgov.be