

Targeted monitoring

Privacy aspects of client monitoring systems and other forms of data exchange

Summary

In bygone days it was quite normal for the friendly neighbourhood policeman to go down to the Voogdijraad, the forerunner organization to the Dutch Child Protection Council, or Pro Juventute, an organization where parents could request supervision of their wayward children, and have a little chat with the ladies who worked there and were regular guests at the houses of the young clients' parents. The organizations for which these ladies worked have since been completely transformed and the social context of their work cannot be compared to the structures which exist today.

What remains unchanged, however, is the need to coordinate activities and to be informed about what each party is doing with regard to a client. To what extent is this need impeded by the protection of the client's personal privacy? Answering this question requires careful consideration of various needs and interests, of which the protection of the individual's personal privacy is just one. In the Dutch Data Protection Act (Wet persoonsregistraties - WPR, the predecessor of the WBP), the Data Protection (Police Files) Act (Wet Politieregisters - WPoIR) and the decrees based on these laws, rules are laid down for the assessment of these needs and interests. These are general rules which in practice have to be specified more precisely. In some cases, certain legislation may apply directly or have to be adapted on the basis of the WPR and WPoIR. It is of primary importance to keep in mind at all times the fundamental principles on which the regulations are based.

The various points of interest as regards these issues have been discussed in detail in the previous chapters and shall be summarized here, with references to the section of the report which dealt with the respective subject.

Points of interest

May the data which various organizations possess about the same client be combined in one file? The purpose of the registration determines whether personal data may be stored in a personal registration system and how they may be used. Since the purpose is the decisive factor for determining how a registration system should be set up and used, it is essential that that purpose is clearly and accurately described.

The purpose determines which personal data an institution or organization may record, i.e. the personal data which are necessary or important to serve the organization's purpose. Qualifications such as 'necessary' and 'important' are open to interpretation and must be more clearly defined. Proportionality and subsidiarity are key concepts for this defining process. If an organization wants to find out whether or not it is allowed to exchange client data with other organizations or make such data available to them, the answer will depend primarily on its own task.

The content and scope of the task determine the organization's purpose. These can then be compared with those of other organizations in order to establish whether they have similar aims and whether joint action is needed to reach those aims, and whether, or to what extent, the exchange of client data is necessary and permitted for that purpose (see chapter 5.1). Data which are stored in a registration system must have been collected by legitimate means. Unlawful collection of data is generally the result of unlawful disclosure, i.e. disclosure for which there was no authorization.

May data about a client be disclosed to a client monitoring system or another organization? And if so, which data? And to which organizations? Does it matter in such cases what the reasons for such disclosure may be? Article 11, Section 1, of the WPR specifies three reasons for permitting the disclosure of personal data in a personal registration system (see chapter 5.1.3).

Legal obligation

It may be that a law contains the obligation to disclose certain data. Such a legal requirement has to fulfil a number of conditions.

Consent

It is also possible that the client consents to the disclosure of certain data about him or herself to third parties. Consent to the disclosure of personal data is also subject to certain conditions.

Purpose

In the absence of consent or legal obligation to disclose data, authorization to disclose them may exist nevertheless if this logically ensues from the purpose of their registration. The purpose of a registration system of personal data is therefore also important for determining whether data from that system may be disclosed to another organization. Disclosure 'logically ensues' from the purpose of data registration when the purpose of a certain registration system necessarily gives rise to the disclosure of data to third parties. The notification or rules of procedure for a personal data registration system require a specific description of its purpose. This description, however, may still provide insufficient information to determine whether disclosure of certain data logically ensues from that purpose, for the purpose may be described in very broad, general terms.

In such a case the purpose of the registration system needs to be specified in more precise terms. The relationship with the data subject and the type of registration may provide the necessary clarification of purpose. Did a degree of dependency play a role, for example? Was the data subject free to disclose or refrain from disclosing the data, or was there indeed an obligation, or were the data obtained via third parties? Could the data subject expect such disclosure of data to take place, or should some degree of confidentiality be considered normal in cases involving this kind of relationship, this kind of data or this category of data administrator?

The relevance of a registration system's purpose in society and the relationship between a data subject and the administrator of such a system can change in time or as a result of evolving circumstances. The same applies to the issue of whether specific disclosure of data is part and parcel of the purpose of a registration system. This often depends on several factors. In some cases, interpretations within a certain branch or profession, or the data subject's expectations due to established patterns may play a role. The interest of the data subject, i.e. the protection of his or her personal privacy, must be duly considered in matters of data disclosure. This can entail ensuring that the data subject has the right to appeal against the disclosure, or at least that the data subject is informed of such a disclosure. Disclosure of data cannot be considered as logically ensuing from the purpose if the receiving party obtains more data than it needs. Disclosure of more data than are necessary is in such cases unlawful.

Disclosure to other (semi-)public bodies

For registration systems managed by public and semi-public bodies, Article 18, Section 3 of the WPR contains a possibility to disclose personal data upon request to another (semi-)public body which needs those data in order to accomplish its task. It is however essential to verify that disclosure of the data will cause no disproportionate damage to the personal privacy of the data subject.

Professional secrecy and closed regime of disclosure

Although disclosure of personal data is in principle permitted under Article 11, Section 1, or Article 18, Section 3, of the WPR, it may be that other legislation or regulations within a certain profession stipulate that the person providing the service or care is obliged to treat the client's data confidentially and refrain from disclosing them to third parties without the client's consent. This is known as the legal obligation to secrecy, or professional discretion. In such cases, disclosure of data is only possible if it is specifically provided for in a treatment agreement or if

the data subject gives his or her consent (5.2.1). The disclosure of personal data can also be subject to extremely strict rules, as is the case with data disclosure by the police (5.2.2).

Can care providers or police officers who have received data from another organization use these data at their own discretion with regard to the data subject? Does this also apply to the data they themselves disclose?

The use of personal data within the data administrator's organization must be 'compatible' with the purpose of the registration (see also paragraph 5.1.3). This does not mean that the data may only be used for that specified aim. A degree of leeway does exist, but it has limits. These limits are determined by the term 'compatible' and they apply even if the administrator of a personal registration system records personal data for various purposes, in which case the purposes must be mutually 'compatible'. In the case of a (semi-)public body, the purposes relate to the task of that organization. If an organization participates in a client monitoring system or another form of data exchange for the performance of one of its tasks, it will receive personal data to serve that purpose. Use for other purposes is only permitted if that use, and the tasks concerned, are compatible with the purpose for which the data were originally recorded. What constitutes 'compatible' can depend on various factors. In this context, the Dutch Data Protection Act (*Wet bescherming persoonsgegevens* - WBP) lists the following: the relationship between the purpose for which the data were obtained and the intended (further) processing, the type of data, the way in which they were obtained, the consequences which the intended processing has for the data subject and any safeguards which have been put in place

Who is actually responsible for the whole procedure? Who can be held to account when mistakes are made?

The WPR and legislation yet to be passed contain standards, rules and obligations which have to be complied with. This presupposes that a natural or legal person takes certain decisions, is responsible for those decisions and can be held accountable in case of error or negligence. When institutions exchange data, each institution is individually responsible as administrator for the recording of data, the disclosure of data to other institutions and the use of received data within the institution. There must be grounds and authorization for each of the data processing procedures. This also applies if the exchange takes place by means of an independent database or another type of personal data registration system. For such cases of separate registration, the various responsibilities must be clearly regulated, whether it be that a specific legal person or one of the organizations accessing the data is responsible as the administrator, or that each of the parties accessing the data is responsible for its own part of the registration system (chapter 4.4).

Duties of the administrator

The administrator of a personal data registration system, or the party responsible for the processing of data, has the duty to notify the Dutch Data Protection Authority (DPA) of the registration or processing. If several administrators of personal data registration systems exchange data on a regular basis, the Dutch DPA must receive a notification or the rules of procedure governing the disclosing and obtaining of data which result from this exchange.

The administrator must also ensure that the data system which he sets up fulfils certain quality requirements. He does not have to guarantee that every item of data in the registration system is correct, but he does have to ensure that the data are as accurate as possible. 'Accurate' in this context means more than 'not inaccurate'. The data must also be sufficient, relevant and not excessive in relation to the purpose for which they are being processed. The data must also be precise, and, if necessary, be updated. In this context all reasonable measures must be introduced to delete or correct data which are inaccurate or incomplete.

Furthermore, the administrator must take the utmost care to ensure that the data are not lost, distorted or made accessible to unauthorized persons. The greater the interests which are at stake and the greater the risks presented by the use of certain data, the greater the efforts which can be expected of the administrator to provide efficient data protection.

What influence can the client exert on the processing of his or her data? What exactly should the client know, and when?

The person with the greatest interest in compliance with the substantive standards and obligations of the WPR is the registered person, or data subject, to whom the WPR therefore accords a number of rights. The data subject must be able to know which organizations record his or her data, for what purpose they do so and to whom the data are being disclosed. The administrator or responsible party is obliged to make this information available to the data subject, either when the data are recorded in the registration system or later, should the registered person request such information. Data subjects also have the right to request correction or possible destruction of data if these are incorrect. Should data subjects wish to exercise these rights, it must be clear to them where to address their questions. If organizations exchange data about clients, there must be clear agreements to regulate such procedures. After all, the situation must not arise in which the clients' rights are frustrated by precisely those initiatives which were designed to serve their interests (see chapter 5.4).