

## Your Data on a Black List

This fact sheet is intended for the *data subject*, i.e. the individual whose personal data is being used.

THIS FACT SHEET WILL ANSWER THE FOLLOWING QUESTIONS:

What is a black list?

Does the Dutch Data Protection Act apply?

Which conditions apply to the use of black lists?

Which conditions apply to the creation of black lists by specific sectors?

Should the Dutch DPA be notified of black lists?

When should prior investigations be requested?

What can you do if you would like to know more or have a complaint?

Which other rights do you have?

Number 22B, November 2006

The titles in italics are also available on [www.cbpweb.nl](http://www.cbpweb.nl).

Various companies and sectors may have a legitimate interest in your inclusion in a black list. Black lists are permitted in the battle against misconduct and fraud. The Wet bescherming persoonsgegevens (Wbp) [Dutch Data Protection Act] lays down the norms applicable for the creation of black lists. Without proper safeguards, black lists are prohibited.

### **The definition of a black list**

A black list is a warning or detection list: the registration of individuals created by a company or sector. For example, an airline may have a black list to ensure that difficult passengers are prevented from using its flights. The worst offenders are banned from flying for a minimum of five years. Another example of black lists are those maintained by banks and insurers, which maintain an incident register recording actions on the part of (legal) persons that have resulted or could result in damage to financial institutions.

The object of a black list is to have access to your personal data that a company or sector believes are essential for the proper assessment of the individual with whom a contract will be entered into. Some offences will be considered more serious than others in this test of necessity. For example, an applicant may be found to appear on a black list of employees that have committed minor offences. The future employer should then contact the former employer in order to gain information on the reason for the applicant's dismissal, enabling it to decide whether or not to recruit the applicant. Automatic exclusion 'by the computer' is not permitted.

### **Applicability of the Wbp (Dutch Data Protection Act)**

If you are on a black list, the Wbp will apply. This Act pertains to the fully or partially automated processing of personal data, as well as to non-automated data that have been or are to be added to a file. Personal data comprise all data relating to an identified or identifiable natural person. In practice, the black lists maintained will virtually always be automated, facilitating their use by authorised (legal) persons. Where you are on a particular black list, the data held on you will be personal data, and will contribute to the way in which society assesses or treats you. As such, the personal data used for black lists must be processed properly, with all due care and in accordance with the provisions of the Wbp.

### **Conditions applicable to the use of black lists**

If a company is planning to create a black list, it must be able to prove its legitimate interest in a list of this nature. The processing of your data must be essential for the company's legitimate interest. The company must be able to demonstrate that the purpose for which the black list is required (the prevention of employee fraud, for example) cannot be achieved by any less drastic means. The data subjects in question may be employees, customers or suppliers.

In addition to the above, the company must also be able to demonstrate that its business interests outweigh your privacy interests. The company will be expected to consider the seriousness of the offences involved and the consequences arising for you from inclusion in the black list.

### **Black lists in specific sectors**

If the black list is made available to (a considerable part of) the sector, there must be an important interest justifying the major infringement of your privacy. Since this type of system has far-reaching consequences for you, more stringent safeguards must be put in place to guarantee careful use and to protect your rights. Amongst other things, this means that the criteria applicable for inclusion on a sector-wide list should be tightened up. For example, only those employees who have committed very serious criminal offences will qualify for inclusion in a broad warning list of this nature. In short: the greater the consequences for the data subject, the more stringent the criteria applicable must be.

Please see the document entitled *Checklist Zwarte Lijsten* [Black Lists Checklist] for information on other criteria to be taken into consideration. All publications by the Dutch Data Protection Authority (Dutch DPA) [College bescherming persoonsgegevens (CBP)] on the subject of black lists are available from the theme file *Zwarte Lijsten* [Black Lists].

### **Obligation to notify the Dutch DPA**

The Dutch DPA must be notified of a company's intention to create a black list. The controller must notify the Dutch DPA of all personal data processing. Under the Wbp [Dutch Data Protection Act], the controller is the individual that determines the object of and or the resources available for processing. A third party is also able to effect notification, provided this occurs on the controller's behalf. In situations where there are a number of controllers, notification must be made by or on behalf of each controller separately. In practice, one of the controllers will be able to act on behalf of the other controllers. For more information, please see the fact sheet entitled *Melden en Vrijstelling* [Notification and Exemptions].

### **Prior investigation**

If an organisation is planning to process criminal data or data relating to unlawful or objectionable behaviour for use by third parties, the Dutch DPA will have to conduct a so-called 'prior investigation' in some situations. Third parties will be understood to include the participating companies within a sector. During a prior investigation, the Dutch DPA will ascertain whether the interests of the sector in a black list can be justified and assess whether or not adequate safeguards are in place. For more information, please see the fact sheet entitled *Prior Investigation* [Voorafgaand onderzoek].

### **If you have any questions or complaints**

Your first course of action should always be to contact the organisation itself about your questions or complaints. For information on your right to access to your data in the event of a dispute, please see the fact sheet entitled *Mediation by the Dutch DPA in Respect of Your Data* [Bemiddeling door het CBP inzake uw gegevens]. If you believe that your personal data have been used wrongfully and the controller fails to respond to your complaints, or fails to respond to your satisfaction, please refer to the fact sheet entitled *Your Complaint and the Dutch DPA* [Uw klacht en het CBP] for information on the subsequent actions open to you.

### **Your rights**

It is important for you to know whether or not you are on a black list and, if so, which data have been registered. As soon as your data are collected, the controller must inform you of his name and address and the reason for his collection of your data. Often, the controller will also be required to state any other particulars, so that you know exactly how he plans to use your data. Please note that the controller will not be required to provide you with the above information in situations where you are already aware of said information, or where it is essential, in the interest of the prevention and investigation of criminal offences, that this information is not provided. Added to the above, the controller must ensure that adequate (organisational) measures are in place for you to be able to exercise your right to access your data and/or request their correction. Clear agreements must also have been made as regards the length of time an individual's data will remain on the black list. For more information, please see the fact sheet entitled *Data Subjects and Their Rights* [Rechten van de betrokkene].