**11118/02/EN/final**
**WP 65**

# Working Document on Blacklists

**Adopted on 3 October 2002**

# BLACKLISTS

## THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],

having regard to Articles 29 and 30 paragraphs 1(a) and 3 of that Directive,

having regard to its Rules of Procedure and in particular to Articles 12 and 14 thereof,

**has adopted the following working document:**

The Working Party first recalls that a person's right to the protection of his personal data is a fundamental right laid down in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. It is also enshrined in the Charter of Fundamental Rights of the European Union and elaborated upon in Directives 95/46/EC and 97/66/EC on the protection of personal data.

The fundamental right to data protection, as an independent right autonomous of the right to privacy or the right to communications secrecy, in practice represents a starting point and an innovation in our society. The need to strike the right balance between this and other fundamental rights, in one hand, and other legitimate public and private interests with individual and general repercussions, in the other, combined with technological progress of the significance and scale to which we are witnesses and which make it possible to disseminate, to store and to process enormous quantities of information in little time and at negligible cost, demand consideration of a highly important aspect of the position of a great number of citizens in circumstances which can lead to conflicts (virtually all of which are undesired) in the progress of commercial, financial, professional or private dealings.

Entering individuals onto databases on which they are identified in connection with a specific situation or specific facts represents an intrusion. This increasingly common phenomenon is currently known as “blacklists”. They are hard to define for various reasons given that, quite apart from the difficulty of uniformly determining their concept and nature, it is also necessary to consider the differences caused by the different laws and legal and constitutional traditions, which exist in every Member State[2].

Taking a generic approach to a possible basic concept, a blacklist could be said to consist of the collection and dissemination of specific information relating to a specific group of persons, which is compiled to specific criteria according to the kind of

[1] Official Journal L 281 of 23.11.1995, p. 31, may be consulted at: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

[2] It should also be noted that in some Member States, data protection legislation is also applicable to legal persons

blacklist in question, which generally implies adverse and prejudicial effects for the individuals included thereon and which may discriminate against a group of people by barring them access to a specific service or harming their reputation.

Given that any operation or set of operations applied to personal data, whether carried out by automated procedures or not, constitutes processing of personal data subject to Directive 95/46/EC and is, therefore, subject to the respective rules transposing this in the various Member States, for these so-called blacklists to exist legally, they must be subject to the principles of legitimacy set out in that Directive and must uphold the rights which it confers on citizens unless they qualify for any of the exceptions provided therein.

This document was drawn up on the basis of the information provided by the supervisory authorities of the European Union Member States following internal consultation among the members of the Article 29 Working Party which identified the main categories or kinds of blacklists and their most striking features. The consultation showed that certain kinds of regulated "blacklists" are widespread. These are records of debts and criminal offences or relate to fraud prevention, and they all have some kind of legal basis in different national regulations.

Other kinds of "blacklists", which are not as common as the above-mentioned ones do exist, and the regulations governing them are far from uniform. The most significant include those concerning administrative offences, professional misconduct, employment records or files containing information on specific individual conduct which certain social sectors find inappropriate.

**Debtor records and solvency and credit information services**

This kind of file is perhaps the blacklist, which has most bearing on a great number of citizens, and is found in every Member State. The processing of personal data generally occasions the greatest number of complaints to European data protection supervisory authorities. The first point to be made concerning these records is that every Member State provides various kinds of regulations. In some cases, these are contained in the regulations transposing Directive 95/46/EC, while in others they feature in rules governing the commercial or financial sectors. Rather than assessing or judging the legitimacy of these files which do, as said, have a legal basis in the respective Member States, this document aims to analyse how they are brought into play and operated in practice.

These activities entail consultation among discrete undertakings in order to pool, generally via a central body, customer information with a direct and significant bearing on commercial or service conditions. The legal regulation of these lists is based on the undertakings' need for information permitting them to assess risks when agreeing to provide a service or to deliver goods on credit and thus fulfil the function of stabilising and ordering trade operations.

A clear distinction should be made between records, which are styled solvency and credit information, and those intended to provide information on the breach of monetary obligations.

The former serve to assess a person's economic and financial capacity to assume a future credit commitment. The latter store data on compliance with or breach of monetary obligations with the aim of establishing whether an individual has failed to meet previous obligations. These entail a negative rating for subsequent credit, of course.

With files containing a positive record of a person's payments (which are forbidden in certain Member States, given that a debtor's meeting his obligations does not represent any risk whatsoever for the stability of the financial system nor, in principle, is the communication of this information necessary for successful contractual relations between the parties), including these data on joint files should have its basis in legislation providing for this course (e.g. making it possible for the competent financial authorities to assess the general risk assumed by financial concerns) or in the data subject's free, unequivocal, specific and informed consent.

In any case, this kind of file is mentioned here because it should be borne in mind that while, unlike blacklist files, such a positive background file is not maintained with any aim of stigmatising a group of people, their widespread use would have the same effect by a kind of positive discrimination (*anyone on the list is good, anyone who is not is bad, or at least suspect*).

A distinction should also be made between two kinds of files relating to the breach of monetary obligations:

> The first is a **creditor's file**, which records all payments by a specific debtor, and arises from the creditor's contractual relations with the debtor. The second is a so-called **joint file**, the data controller for that is a body which provides solvency and credit rating information to which the creditor supplies the data. These are known as "bad debt files". Generally, several bodies (sometimes within a single sector, sometimes covering a broader spectrum) enter into an agreement with a third undertaking pursuant to which they agree to communicate the records of customers who default on loans to that undertaking, whereupon this information is incorporated into the joint debtor file which the data controller makes available to the parties to the agreement for use in assessing the different credit options available to them.

This kind of file, which is especially relevant because it shares and centralises information and access thereto by the participating entities or companies, constitutes a real blacklist of persons who have failed at any time properly to meet their previous financial commitments. The legitimacy of including information on it must be based either on the existence of specific contract clauses authorising the creditor to disclose the data on the outstanding debt to a joint file or — and this is fundamental — on the data controller's legitimate interest in knowing whether anyone applying to it for credit has a record of failing to repay a loan.

It is therefore this legitimate interest in the preservation and stability of the financial system which justifies the communication of this information to third parties, although this course, which has serious adverse effects for the data subject, must be taken without losing sight of the principles of the Directive, and specific safeguards must also be in place to uphold data subjects' legitimate rights.

This balance of interests therefore demands that the dissemination of data, which may have adverse effects for data subjects, should be subject to a series of requirements and safeguards which are laid down in the Directive and in Member States' regulations.

a) First, the principles relating to data quality contained in Article 6 of the Directive must be observed. Basically, this means that a definite due debt must have remained unpaid, and the debtor responsible for meeting this obligation must have received a reminder requiring him to make the payment.

   The information incorporated into the file must be accurate and up to date. For these purposes, the retention or erasure of an entry in respect of a specific debt once it has been paid becomes highly relevant. In this regard, although an element of criterion is to be seen in the need to limit the time for which negative data remain on these files, it should be stressed that there is no unanimous view on how long this period should be, and the various Member States have taken different approaches to this problem. In some, this entry may not be maintained once a debt has been paid off, even when overdue, while in others the information may stay on record for a maximum period which varies from one country to another[3]. Notwithstanding these divergences, what is clear is that the principle of updating information entails an obligation clearly to reflect the fact that the debt has been paid off even if the entry on non-payment is maintained beyond the date of full repayment.

b) Data subjects, as they do not report the debt for inclusion on the joint file, should be provided with the information specified in Article 11 of the Directive since the very moment of the inclusion of their personal data in the common file. For this information to be correct, every reasonable step should be taken to guarantee that the data subject receives notification. This notification safeguards their right to defend themselves and thus avoids any errors (e.g. in identifying the data subject or including debts, which the data subject is not paying because he disagrees with the amount or with the service provided).

c) Another aspect of capital importance is the need to guarantee the full range of citizens' right of access to the data on these files and the right to have them corrected or erased when the information contains errors or data which should not appear on the file. Obstructing or denying these rights (e.g. sending citizens on a tour of several data controllers or offering them incomprehensible information) is unacceptable practice which hampers the necessary transparency and operation of these files. Therefore, a sole interlocutor able to furnish all the relevant information and to deal with the exercise of the rights by the data subjects should be appointed when notifiying the inclusion of the personal data to the citizen.

d) A further important aspect of this kind of file concerns individual automated decisions referred to in Article 15 of the Directive. Given the prevalence in financial concerns of computer programs for assessing individuals credit worthiness ("credit scoring"), the need to recall the safeguards in Article 15 is imperative. These safeguards underpin a person's right not to be subject to this

[3] Sometimes, the retention period is also set in the contractual arrangements between the creditor and the debtor even though it cannot go beyond this maximum period.

kind of decision, other than as provided for by law, unless the decision were taken at the data subject's request when entering into or performing a contract or unless there are provisions permitting him to defend his legitimate interests, such as defending his point of view, for example.

It should also be recalled in relation to this kind of decision that Article 12 of the Directive establishes citizens' right to know the logic used in any automated processing leading to this kind of decision.

**Criminal offences**

Article 8(5) and (6) of Directive 95/46/EC mention the processing of data relating to criminal offences or criminal convictions[4], and lay down that, generally, such processing may only be carried out under the control of official authority unless the Member States adopt exceptions which must have adequate safeguards in order not to affect citizens' fundamental rights and must also be notified to the European Commission.

The legitimacy of processing the kind of file, which incorporates data on criminal offences, centres on the obligation on authorities to maintain security and public order. Beyond any doubt, this principle justifies such processing provided that the restrictions mentioned in the preceding paragraph are observed, as provided by Article 7(e) of the Directive.

As regards the processing of personal data relating to criminal offences, most Member States have files incorporating this kind of information which are controlled by an official authority.

This notwithstanding, various supervisory authorities have found that files with these characteristics are created and managed privately in their countries and refer, essentially, to files existing in large supermarkets or in vehicle rental firms. When supervisory authorities have detected cases of personal data on “undesirable customers” being collected and processed in supermarkets, hypermarkets or department stores, they have instructed the data controller to end such processing because it is inadmissible for private companies to keep this kind of file.

This kind of processing must always uphold the data quality principles contained in the Directive, and those on accuracy and up-to-dateness in particular. Likewise, special attention must be paid to the right to routine or automatic correction and erasure of a

[4] Article 8 of Directive 95/46/EC: *“(...) 5.Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority. Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.*
*6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission”*.

subject's data once the time provided by law has passed and to marshalling to this effect the various mechanisms which make this possible, easier and prompter, given that the retention of information referring to a person on these files beyond the periods laid down can have prejudicial consequences.

This is especially relevant with not guilty verdicts, limitation of liability or the discharge of bankrupts. There would be no point in retaining such data. It should be noted that most Member States regulate these aspects under the respective criminal law, and the criteria laid down to this effect vary.

Another fundamental point, which must be considered, is access to information, i.e. determining which persons or institutions are entitled to access the data included on these files. Data subjects must also always have the right of access to the information concerning them on a file.

This access provision can give rise to somewhat complex and problematic situations, such as when the data subject is a job seeker in that, in those Member States in which it is permitted, as part of the selection process, an employer could ask a worker to produce the contents of a certificate of any criminal record issued by a public authority data controller. The candidate would obtain such a certificate, which could contain data on any criminal convictions or other security measures. The employer thus gains access to the content of certain data which is not directly legally recognised.

This hypothesis can be further complicated in situations which may arise as a result of the employer's subsequent use of this information, given that, in principle, simply consulting the information made available by the candidate during the selection process would not be in breach of the provision of Article 8(5) of the Directive, whereas any subsequent manual or automated processing could be.

**Fraud detection**

In certain sectors of the economy, and essentially the insurance sector, attempted fraud can be so frequent and can have such a bearing on companies' activities as to have them set up sources for communicating information via joint files which help them to combat fraud techniques and thus to reduce their operating costs.

Joint or centralised files fed by information available in the companies[5] are used to post information on payments made to clients suspected of fraud or action in breach of the provisions in force relating to the sector concerned[6].

[5] See paragraph 2 of the section on debtor files and solvency and credit information services.

[6] In some countries, insurance companies also centralise information on clients considered as presenting specific risks, using criteria such as e.g. the number of damages related to a client in a certain period of time, without always taking into account the responsibility of the client in the damage. The justification of insurance companies is that such number of damages, even without responsibility of the client, might be considered as a preliminary element to presume fraud. The non compliance of some aspects of this kind of processing with data protection legislation, unless legal provisions specifying adequate guarantees under National Law exist, has been pointed out by some data protection authorities.

Given the similarities which exist between both (centralised files, communication of data by third parties, dissemination of information between the parties to the system, etc.), both the problems and the various safeguards to be put in place are similar to those for files on breaches of monetary obligations or "bad debt files" examined above[7].

Such lists must be set within a legal framework of compliance with the regulations on personal data protection: exercise of the right of access, notification of the data subject on his inclusion on this file[8], conservation of the data for a period commensurate with the purpose for which they are collected and the obligation to erase data when they are no longer necessary for the purpose for which they were compiled.

Another important question is the importance of providing mechanisms necessary to avoid errors in identifying the individuals included (which is especially relevant in the case of data subjects with common names) in including wrong debts (e.g. debts under discussion with the data subject) and in references to the amount of debts, errors in updating these in the event of subsequent payments, etc.[9] Any error of this kind must immediately be corrected as soon as it is detected, which implies setting up rigorous verification instruments. In most countries, this kind of file is private and, where the internal regulations in the various Member States are concerned, it should be pointed out that data subjects are generally informed that they have been included on a file, as required by rules to this effect, although the information given to the data subject may not always be complete and exercising the right of access may on occasion prove difficult because of the complications the subject may face.

**Other categories of blacklists**

Having quickly looked at the categories of "blacklists" which are most uniformly distributed and regulated in the Member States and on which most information is therefore available, another group, while hitherto not as prevalent and regulated, is no less important in view of the enormous impact it may have on the lives of persons included on them. Noteworthy files in this category contain adverse data on employees or job candidates or relate to health questions, social or political behaviour and professional misconduct.

This includes those blacklists based on the collection and dissemination of data which enjoy special protection because they have the greatest bearing on data subjects' interests and it appears that it is with these that supervisory authorities most often have to deal.

---

[7] The legitimising principles are similar: the existence of public interest – combating fraud, the stability of the financial system, regulating and protecting trade operations, etc. - or the data controller's legitimate interests, provided that the data subject's interests or rights and freedoms do not prevail.

[8] One way of avoiding errors and problems would be to lay down a reasonable period between notification of the data subject and the actual entering of the information on the joint file, and this procedure could also apply to files on breaches of monetary obligations.

[9] This point may also be applied to the categories of blacklists analysed in this working document, bearing each one's special distinguishing features in mind.

These are regulated by Directive 95/46/EC, Articles 8[10], 13 and 15[11]. Most Member States, in accordance with the Directive, ban the processing of special categories of personal data without the data subjects' explicit consent.

Some provide for the processing of this kind of data if it is authorised by law or if there are legitimate public or commercial interests at stake[12], given that the Directive provides that Member States may lay down other exemptions providing grounds for processing especially protected data subject to the provision of suitable safeguards[13]. Similarly, some Member States operate an express legal ban on the compiling of blacklists of workers.

In some Member States, in fact, the courts have proscribed the compilation of files containing data on political opinions, trade union membership, ethical questions or information on workers' health. Courts have censured this kind of file even when, in the cases mentioned, they were solely to be created within the bounds of the firm.

As for blacklists including any other kind of especially protected data, such as health information, it should be pointed out that files of this kind on such questions are essentially compiled in connection with life insurance offered by companies in that

---

[10] Article 8 Directive 95/46/EC: "1. *Member States shall prohibit the processing of personal data revealing racial or ethnic origin, **political opinions**, religious or philosophical beliefs, **trade-union membership**, and the processing of data concerning **health** or sex life.*
2. *Paragraph 1 shall not apply where: a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or*
*processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorised by national law providing for adequate safeguards; or*
c) *processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent,* [...];
*3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy".*

[11] Article 15 Directive 95/46/EC: Automated individual decisions: "1. *Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.; 2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision: a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or : b) is authorised by a law which also lays down measures to safeguard the data subject's legitimate interests".*

[12] See Article 8.2b) of Directive 95/46/EC.

[13] Article 8(4) of Directive 95/46/EC: Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

sector. In such cases, in the absence of legal regulations incorporating the appropriate safeguards, these files may only be compiled with the data subject's free, specific, explicit and informed consent, which he is entitled to revoke. Even then, however, Article 6 of the Directive must be taken into account, as must, in particular, the proportionality of creating these files in relation to the end in sight. It is also necessary to establish that no specific rules in the Member State concerned prohibit this kind of practice even when the data subject has given his consent.

The restrictions on automated individual decisions provided by Article 15 of Directive 95/46/EC should again be recalled.

As specific examples of action in relation to this kind of blacklist, some national supervisory authorities have reprehended joint files centralised by a federation of insurance companies which included data on persons who had been refused life insurance on the grounds of their health problems. The supervisory authority ruled that these had to be deleted or legitimised in accordance with the Directive, as it took the view that it was not sufficient that this information should be available to the respective companies with life insurance contracts with those data subjects with which the nature of the contractual relations could provide grounds for holding this information.

Blacklists including especially protected data referring to certain activities with social or political repercussions are solely admissible and do, in fact, exist in some Member States (registers or public files of persons whose conduct is considered dangerous) when the legal provisions for compiling these also specify the safeguards and the restrictions on access to the data. Lastly, and on similar lines, although there is widespread agreement among the supervisory authorities that these lists are not legitimate, some Member States have seen conflicts between the right to privacy of individuals appearing on these lists and the right to freedom of expression of those circulating them; courts have favoured the latter right in some specific cases in some Member States and overruled it in others.

While this document is not intended to analyse legal decisions or to make a blanket ruling on where the balance is to be struck between these rights, it needs to be recalled that, even though in very specific cases and by virtue of legal and constitutional traditions in which the right to freedom of expression is given a very broad interpretation, this is no impediment to respecting the principles of scope, proportionality, the data on these files being up to date and exercise of the right of access, the right to rectify and to erase data. If these are refused, the data protection supervisory authorities are bound to offer an opinion.

## CONCLUSIONS AND RECOMMENDATIONS

As stated in the introduction, this working document aims to highlight the phenomenon of blacklist files in the European Union by describing the situation which exists in the light of the information provided by the supervisory authorities of the Member States of the European Union in internal consultation between the members of the Article 29 Working Party.

The analysis made herein points to two fundamental conclusions: the incidence, prejudicial effects and consequences of this kind of joint file for individuals' private (and social) lives, and the existence of clear discrepancies in how this kind of file is regulated and used in the Member States.

Generally, therefore, it is important to emphasise the case for having uniform, harmonised criteria[14] for the processing of personal data known as "blacklists" which provide formulae to guarantee that data subjects can exercise the rights recognised in the rules protecting the right to privacy and personal data. In the light of this document, this harmonisation is especially relevant in relation to the following issues.

The importance of determining mechanisms which clearly and transparently define the kind of personal data which are likely to be processed, the purpose of such processing and the safeguards available to data subjects (i.e., establishing systems of checks and controls for the information which is processed) and the circumstances and the preconditions which render such files permissible. This should be set out within the framework of the principles by which processing becomes legitimate contained in Article 7 of Directive 95/46/EC.

Updating information is also fundamental[15]. It would be very useful to try to define general parameters for standardising the times for which the data contained on files may be kept or blocked. The lack of transparency in relation to this data quality principle enshrined in the Directive may leave data subjects totally unprotected for lack of mechanisms which can subsequently make good the injury caused (i.e. in the event of the communication of data to third parties without the data subject's knowledge).

An effort to achieve the maximum harmonisation on this question would go some way towards eliminating the different criteria which exist at present in most Member States, and would facilitate economic operators' work within the framework of the competition law, in line with Recital 7 of Directive 95/46/EC [16].

---

[14] Within the framework of Directive 95/46/EC and the respective national laws.

[15] Article 6.1.d) Directive 95/46/EC: Principles relating to data quality: "1. Member States shall provide that personal data must be: [...] accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified". See "Debtor records and solvency and credit information services" above.

[16] "Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number

Another crucial aspect is data subjects' right to be informed on the processing of their personal data. Breach of this cardinal principle leaves citizens vulnerable in that they have themselves no knowledge that their personal data have been entered on a blacklist because these were obtained from another source, which prevents them from effectively exerting the rights of access, rectification, erasure and objection[17].

Proper regulation of the procedure for notifying data subjects is essential, including criteria on timely information in due form, and a clear statement of any conditions on which data may be divulged to third parties[18].

Mechanisms could also be provided to include the information given to a data subject when he is denied a specific service and any provision for subsequent checks by the subject (within the framework of the safeguards referred to above). In fact, the Directive recognises the data subject's right not to be subject to a decision that produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him[19].

There are also grounds for assessing the case for setting up mechanisms which make it possible for the data subject to intervene and, if he can assert due grounds in any dispute, to call for timely information vouching for his position to be included in the file.

Another key point concerning joint and shared centralised files is the obligation on data controllers to establish and implement the right technical and organisational security measures and conditions of access to such files[20].

---

of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions."

[17] Article 11 Directive 95/46/EC: Information where the data have not been obtained from the data subject: 1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it: a) the identity of the controller and of his representative, if any; b) the purposes of the processing; c) any further information such as: the categories of data concerned; the recipients or categories of recipients; the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject. 2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards." See this document concerning "Debtor records and solvency and credit information services". Those cases in which the information is obtained from the data subject should be recalled.

[18] See Article 11.1 Directive 95/46/EC."Information where the data have not been obtained from the data subject".

[19] Article 15 Directive 95/46/EC "automated individual decisions".

[20] Article 17 Directive 95/46/EC "Security of processing".

As stated, therefore, and given that the existence of files including blacklists in specific sectors providing services of great importance (like the financial or telecommunications sectors) affects a greater number of citizens, the Working Party on the Protection of Individuals with regard to the Processing of Personal Data wishes to raise awareness in all the Community institutions of the need to push ahead on the lines marked out by the conclusions and to emphasise the need for common criteria, guidelines or lines of action in this area, within the framework of and in compliance with Directive 95/46/EC and with the Member States' respective internal laws.

Done at Brussels, 3 October 2002

For the Working Party

*The Chairman*

Stefano RODOTA