Legal Assessment of Issues Regarding the Scanning of Individuals for the V-Man Project

20th October 2003

by Esther Geis,
Matthieu Mélin
& Björn Siepmann

Abstract:

Legal Assessment of Issues Regarding the Scanning of Individuals for the V-Man Project

I. Compliance with UK law

II. Requirements of UK data protection law

III. Comparison of German and UK law

IV. Applicable law

V. Analysis of the Rights of a person on his/her own image (EU context)

Content

1 Compliance with UK law

In order to process the 3D images in question lawfully the 3D-MATIC laboratory has to comply with certain UK common and statute law requirements as well as with data protection law.

1.1 Common and statute law requirements to be observed by the laboratory

The processing must not infringe common or statute law, neither civil nor criminal[1]. As to common law this includes in particular; breach of confidentiality, the ultra vires rule or legitimate expectation. In this respect no problems are obvious.

Breaches of statute law for example include infringements of the Computer Misuse Act 1990-e.g. by obtaining data through "hacking" or unauthorised altering/destructing computer based data -, or infringements of the Theft act –e.g. by obtaining data through theft-, and also infringements of the Copyright Data and Patent Act 1988[2].

As long as the V-man project does not act in breach of any of these rules, e.g. does not obtain data through hacking etc, no problems arise in respect of compliance with common and statute law.

1.2 Legal capacity

The Age of Legal Capacity Act (Scotland) sets out 16 as the age of legal capacity in Scotland and specifies that a person under the age of 16 has legal capacity to consent on his own behalf in restricted cases, as long as he is capable of understanding the nature and, possible consequences of the procedure or treatment. However, bearing in mind that a child over 16 but under the age of 18 might set aside the transaction he has done and also in perspective of achieving the greatest possible protection of the child I would recommend the laboratory to only enter into contracts with people not younger then 18, unless their legal representatives have consented to it.

[1] Data protection Commissioner, Legal guidance to the Data Protection Act 1998, p.29.
[2] Jay/Hamilton, Data Protection Law and Principles, pp.51.

2 Requirements of UK data protection law

There are eight data protection principles in the Data Protection Act, which data controllers in general are required to comply with, unless they can claim an exemption.

2.1 Applicability of the UK Act

The UK data protection act applies if "personal data" are "processed" by a controller, who is "established in the UK" and processes data in the context of his establishment.

2.1.1 Responsible entity for compliance with data protection law

The responsible entity for the compliance with data protection law, the so-called controller- is the body, which stores the data for itself or which instructs another entity to do so.

For UK law to apply the controller has to be established in the UK. An individual is treated as established in the UK if he is an ordinary resident in the UK[3]. Since the 3D laboratory is employed by the University of Glasgow it is established in the UK.

If the controller is neither established in the UK nor the EEA but uses equipment in the UK for processing the data other than transferring them through the UK the act also applies, as long as a representative is nominated by the controller who is established in the UK[4].

2.1.2 Personal data

The data in question must be personal data in the meaning of the UK Act. According to the definition in the Act, "personal data" means *"data that relate to a living individual, who can be identified from those data; or from those data and other information, which is in possession of or likely to come into possession of the controller and includes any expression of opinion about the individual and any indications of the intentions of the data controller or any other person in respect of the individual"*[5].

Whether an individual is identifiable depends on the view of the data user[6]. The criterion of identifiability is of course satisfied if data are directly linked to the name of an individual. Whereas an individual may be "identified" without necessarily knowing the name and address of that particular individual, since it is sufficient if the data enable the data controller to distinguish the data subject from any other individual[7].

[3] Jay/Hamilton, Data Protection Law and Principles, p.41.
[4] Section 5 (a) (b) of the Data Protection Act 1998.
[5] Section 1 (9) of the Data Protection Act 1998.
[6] Lloyd, Information Technology Law, p.73.
[7] Data protection commissioner, Legal guidance to the Data Protection Act 1998, p.12.

No specific legislative provisions exist under UK law regulating biometrics as well as sound and image data. Whereas recital 14 of Directive 95/46 EC points out that image data relating to individuals are included in the definition of personal data. The images in question are therefore "personal data" in the meaning of the act, if the information contained in the data can be directly or indirectly matched to a certain individual. Direct identification is given if the identity of the person is either contained in the data or can easily be found out e.g. in case of an identifying number. Indirect identification is given if additional knowledge or external data allow to make a connection between the data and the individual. Whereas where this connection cannot be drawn or where this is possible only under disproportional efforts the data do not fall into the scope of the act.

The V-man project processes 3D images of persons, which are taken from different angles, showing the entire body of the person in great detail from all possible angles. Since the persons to be scanned will enter into contracts with the laboratory their name, address and bank account number therefore will also be known to the laboratory. Even if the 3D-MATIC laboratory would store images and contracts with names etc. separately it is still highly likely that it will be possible for them to find out which image relates to whom. This is not at least the case because the amount of person's that enter into a contract with the laboratory will not be that high that it is impossible for them to remember whose data were processed. Furthermore where data consist inter alia of an individual's face it is presumed that a strong likelihood of identification of the corresponding individual exists[8]. Whereas the existence of personal data is at least doubtful where data consist only of fingerprints[9]. Since the images in question show the entire body of the person a great likelihood of identification exists. As a result the images can be considered personal data.

The images could also be considered "sensitive data". Sensitive data are inter alia data that reveal racial or ethnic origin or data concerning health. Since the images in question show the whole appearance of a person they could also reveal its race and in some cases they might also to some extent reveal its health-condition. For example images of a person's entire body can expose a typical feature of a disease or a physical condition caused by a genetic disorder but at least the body mass index. One could argue that at least the race of a person can always be concluded from his appearance. It is furthermore recommended to interpret the provisions in a way that achieves most protection for the data subject. As a result the data in question should also be considered sensitive data[10].

Consequently the images can be considered personal data in the meaning of the UK Act.

2.1.3 Data of deceased persons

The UK act is only concerned with living individuals and so if the subject of the information is dead, the information is not assumed personal data. Whereas data processing of deceased persons might be treated as personal data, if data also contain information about a living individual, as in the case of genetic data. However since those data will not be processed in the creative media application, no problem arise from this issue.

[8] British Institute of comparative law, ibid.
[9] British Institute of comparative law, ibid.
[10] British Institute of comparative law, ibid.

2.1.4 Processing

The images in question have to be "processed" to come into the scope of the Act. "Processing" means *"obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including- organisation, adaptation,…"*[11]. This definition of "processing" made in the Act is very close to the one of the Directive. It is very wide and therefore encompasses any activity that could be perceived in relation to data[12] from the collection until the erasure of data. Since the images in question are obtained, recorded and transformed into 3D pictures they are processed in the meaning of the UK Act.

2.2 Compliance with the first data protection principle

According to the first principle of the data protection act, data processing has to be fair and lawful[13].

2.2.1 Fair and lawful processing

Data processing under UK law is fair and lawful if at least one of the conditions in Schedule 2 is met, such as the data subject has given his consent or the processing is necessary to comply with a legal obligation. Also under UK law the V- man project in the context of the creative media application could be legitimised, if a valid consent is obtained.

2.2.2 Requirements of the consent

Consent is not defined at all in the UK Act. Guidance as to what amounts to consent is however given from Directive 95/46. According to the directive consent means: *"…any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed"*[14]. The fact that the data subject must "signify" his agreement indicates that there must be some active communication between the parties. This does not necessarily mean that the form of writing is required[15]. Whereas as can be concluded from case law consent can be express or inferred from some relevant action but not from silence[16]. As a consequence UK data protection law relates the form of the consent required to the circumstances and therefore even accepts implied consent as an appropriate form in some cases[17].

Also the other requirements mentioned in the Directive are to be concluded from case law. The requirement that a consent has to be given freely can be drawn from the fact that a consent obtained by coercion or duress is not a true consent[18]. A reluctant consent may be valid if it is voluntary. Relevant

[11] Part I Preliminary 1 (1) of the UK Data Protection Act 1998.
[12] Bainbridge, Data Protection Law, p.49.
[13] Principle 1 in schedule 1 of the Data Protection Act.
[14] Art. 2h of Directive 95/46.
[15] Data protection Commissioner, Legal guidance to the Data Protection Act, p.31.
[16] Attorney General v. Jonathan Cape (the "crossman diaries" case) 1975, 3 All E.R. 484, in Jay/Hamilton, Data Protection Law and Practices, p.39.
[17] Korff, EC study on implementation of Data Protection Directive, p.27.
[18] The Sibeon and the Subotre 1976, 1 Lloyds Rep 293, in Jay/Hamilton, Data Protection Law and Practices,

factors to consider are whether the person protested, or had an alternative, or whether it was independently advised. The requirement that the consent has to be specific means that a consent must not be too general. It is proposed that the particular type of activity that shall be covered by the consent e.g. marketing, duration etc. should be specified[19]. The fact that the consent has to be informed means that no one can consent to something of which he has no knowledge. A consent is e.g. invalid if the person consenting was incapable of understanding the action she/he was consenting to or if the person could not understand the nature of the contract.

For the processing of sensitive data it is required that the consent explicitly has to cover this. What exactly is meant by explicit is not defined in the act. The Directive requires in Art. 7 a for the processing of mere data that the consent of the data subject has to be given "unambiguously". This does not necessarily mean in writing but nevertheless is a rather strict criterion requiring a clear indication of the agreement, whereas mere acquiescence is not sufficient[20]. If this applies already to the processing of mere data it, according to the "argumentum maiore ad minor", has to apply also to the processing of sensitive data[21]. This means that the consent has to be absolutely clear. In particular it should cover the specific detail of the processing, the particular type of data that are to be processed, the purpose of processing and any planned disclosures[22]. It will be complied with this requirement in any case if consent is obtained in writing. Since the V-man project concerns processing of sensitive data the 3D laboratory needs to obtain an explicit consent and should therefore obtain the consent in writing.

As to the information to be provided for the data subject, this has to include the identity of the controller/or any representatives, the purpose of processing and any further information which is necessary, having regard to the specific circumstances in which the data are to be processed. The more unforeseen the consequences the more likely it is that the controller has to provide further information[23].

Finally it has to be acknowledged, that the consent can be withdrawn with impact for the future at any time.

2.2.3 Additional requirements

Obtaining the consent does not necessarily mean that the processing is fair and lawful. For compliance with the criterion of lawfulness the controller must observe all relevant rules of law whether derived from statute or

---

p.39.
[19] Jay/Hamilton, Data Protection Law and Practices, p.39.
[20] Jay/Hamilton, Data Protection Law and Practices, p.40.
[21] Ehmann/Helfrich, EG Datenschutzrichtlinie, p.136.
[22] The data protection Commissioner, Legal guidance to the Data Protection Act 1998, p.31.
[23] Jay/Hamilton, Data protection Law and Practices, p.57.

common law, relating to the purpose and ways in which the data controller processes personal data[24] (see above 2a). The principle of fair data processing sets the requirements as to the method of obtaining data, and hence describes the behaviour between the two parties[25]. To comply with this principle the data subject has to give an informed consent and must not be deceived or misled as to the purpose of processing[26].

2.2.4 Legitimising on other grounds

Under UK law the processing of data is legitimate if this is necessary for the performance of a contract to which the data subject is party[27]. This provision only concerns mere data rather than sensitive data. Hence this rule does not apply in the case of the V-man project.

2.3 Compliance with the other principles of the act

Also under UK law controllers have to comply with certain principles such as, that data shall be adequate, relevant and not excessive in relation to the purpose for which they are processed or the principle that data shall be accurate, kept up to date and not be kept for longer than necessary. Complying with these principles does not match the case of the V-man project and thus does not impose any problems in the given case.

2.3.1 Transfer of data

If data shall be transferred to other entities or to third parties the consent has to be obtained.[28] The data subject therefore has to be informed about any planned transfer of data to third parties and in case of transfer to countries outside the EU/EEA about the conditions/risks of processing. Obtaining the unambiguously consent allows the transfer to countries even if an equally high level of data protection is not ensured.[29]

Without such an explicit consent the data transfer to countries other than the fifteen EU member states and the three EEA member countries (Norway, Liechtenstein and Iceland) is possible under various conditions.

The Commission's decision that a certain country provides adequate data protection is one of them. So far the Commission has recognised Hungary, Switzerland, Canada and Argentina as providing adequate protection. Moreover the US Department of Commerce's Safe harbour Privacy Principles have been considered to provide adequate protection. 3D-MATIC therefore does not need a consent for data transfer to the just mentioned states and to US companies which have signed the Safe harbour agreement.[30]

However as an additional precautionary measure for third-country data transfer, 3D-MATIC should incorporate the Commission's standard contractual clauses[31] into its contract with its customers (entities buying the software). By doing so, 3D-MATIC will be able to adduce an adequate level of protection during third-country

[24] The data protection Commissioner, Legal Guidance to the Data Protection Act 1998, p.32.
[25] Jay/Hamilton, Data protection law and practices, p.53.
[26] First principle Nr.1, Schedule 1 part I of the UK Data Protection Act 1998.
[27] Schedule 2 of the Data Protection Act 1998.
[28] e.g. Schedule 4 (i) Data Protection Act 1998.
[29] e.g. Section 4c (1) BDSG.
[30] list of companies that have signed up to the safe harbour: http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list.

data transfers and the competent supervisory authority[32] is obliged to recognise the contractual clauses as fulfilling the requirements of the Directive for data transfers to non-EU countries that do not provide for an adequate level of protection for personal data. Even if the data subject's consent to the transfer should be considered to be ambiguous, the transfer would then still be lawful.

The usage of the EU's standard clauses will trigger a joint and several liability for 3D-MATIC and the relevant data importer. Any evasion of this clause would severely diminish the data protection safeguards provided for by the standard contractual clauses, and would jeopardise the transfer's legality. The additional basis these clauses grant for the data transfer's lawfulness outweighs this downside though. This is even more so since the scope and applicability of joint and several liability is strictly limited. It only applies to violations of those clauses which produce rights for data subjects and only in cases where it is necessary to compensate individuals for damage resulting from the violation. Pursuant to the so-called mutual indemnification clause, 3D-MATIC would also be entitled to recover from the importer any compensation it has had to pay to the data subject. The general rule is that every party to the contract is responsible for his/her acts *vis-à-vis* the data subject.

In addition to the just stated ways of ensuring the legality of data transfers to non EU/EEA countries the use of binding corporate rules might become another option in the near future. As for now this self-regulatory tool is this under discussion and 3D-MATIC is not advised to rely on this measure due to its uncertain legal protection.

2.3.2 Safeguards to be ensured

According to the seventh principle controllers are obliged to fulfil certain requirements to ensure data security. In particular they shall take *"appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data"*.

In addition to this the controller has the duty to ensure that processors contracted by him observe the above requirements[33]. The data controller is thus responsible for maintaining data security. What measures are appropriate depends on the possible harm that is expected and the sensitivity of the data in question. In particular regard should be had to the state of technological development, the cost of implementing security measures, the nature of the data to be protected as well as the harm that might result from unauthorised or unlawful processing, accidental loss, destruction and damage[34]. A rather high level of protection is for example considered to be achieved by the usage of firewalls and encryption. For guidance the Data Protection Commissioner provides a list of points that should be regarded while deciding on the appropriate measures[35].

---

[31] you can find these attached to this document (**Appendix 4**).
[32] http://www.dataprotection.gov.uk.

[33] Lloyd, Information Technology Law, p.139.
[34] Jay/Hamilton, Data Protection Law and Practices, p.66.
[35] see **Appendix 2**; see also The data protection Commissioner, Legal Guidance to the Data Protection Act 1998, pp.42.

2.3.3 Access rights of the data subject

The UK Data Protection Act access rights according to its sixth principle. It provides that an individual can upon a request made in writing and the payment of a single fee (maximum 10 pounds), obtain information from the controller about; the data being processed, the purposes of processing, the actual or potential recipients of data and, where this is available about the source of his data. This information has to be provided to the individual in an understandable and in a permanent form by way of a copy, unless a permanent form is disproportional.[36] A written request has to be responded within 40 days[37].

The controller however may ignore unreasonable or frequent requests[38]. Moreover the controller can refuse disclosure of information if they fear that this information might enable the data subject to identify another individual from it[39].

2.3.4 Obligation to notify

The Data Protection Act 1998 requires every data controller who is processing personal data to notify unless they are exempt. Exemptions are possible for; maintenance of a public register, some not-for-profit organisations, processing for family/personal or household affairs, processing for staff administration, advertising, marketing, public relations as well as accounts and records. Since the 3D-MATIC laboratory does not fall into any of the exemptions it is obliged to notify.

2.3.5 Damage

Also under UK law damage can be claimed in case of an infringement of any of the above rules.

[36] Government Information Quarterly Vol.16/No.3/1999, p.218.
[36] Government Information Quarterly Vol.16/No.3/1999,p.218.
[37] Kemp Little, www.comlegal.com/Short_Lines/Data_Pro_Privacy_09.htm.
[38] Charlesworth, Government Information Quarterly Vol.16/No.3/1999, p.218.
[39] Charlesworth, Government Information Quarterly Vol.16/No.3/1999, p.218.

3 Comparison of German and UK law

Data processing made in the V-man project is in compliance with both Data Protection Acts, UK and German. Since both countries have implemented the relevant provisions of Directive 95/46 the project is also in compliance with EU law.

Since the laboratory has asked for legal guidance concerning German and UK law, and would choose the place of its office according to the law that is most suitable for it, it has to be considered whether any differences appear in the laws in context of the V-man project. Data processing in the V-man project is not subject to any national prohibitions, such as those incorporated in common or statute law.

Also in case data of a child are obtained both systems do not impose different requirements to this. In particular in both cases consent of the legal representative should be obtained to achieve appropriate safeguards of the child.

As far as compliance of the project with data protection law is concerned only small differences in the acts appear that finally do not even result in different requirements. For example in respect of their scope the two acts do not vary. Both acts apply the same concept to define personal data and in particular treat image and sound data as personal data. As approved before both acts as a consequence of their wide definition of personal data treat the images in question as those.

Moreover both acts apply to the same actions in respect of the matter of processing. They furthermore identify the same person as being responsible for the compliance with data protection. Concerning the legitimising of data processing, both acts only offer the possibility of obtaining a valid consent in the case of the V-man project.

Whereas German and UK law differ in respect of the requirements of obtaining the consent. German law explicitly defines the requirements of the consent in its data protection act and makes the written form to the rule but treats oral and implied consent in exceptional cases. The UK Act fails to define “consent” and therefore does not state anything as to the form that applies to obtaining the consent. However in both approaches the general rule is to be found that, the greater the potential harm to individuals if their personal information is misused, the greater is the responsibility of the controller to ensure that their consent is informed and explicit.

The “explicit” form for the consenting to the processing of sensitive data is required under UK and German law. Since the data processed in the V-man project are considered sensitive data in the meaning of the UK and the German Act, both acts require an explicit consent. What amounts in an explicit consent is neither defined in any of the acts nor in the Directive. However for both acts it has been concluded that it is complied with the requirement of an explicit consent, if consent is given in writing. Hence the same strict requirements apply in respect of both laws. Also as far as the information to be provided for the data subject at/prior to the time of consenting is concerned the laws apply the same strict standards to be observed by the controller. Moreover the rule that consent can be withdrawn applies to both acts. Therefore under both systems the controller has to bear the risk that consent might be withdrawn and data processing become illegitimate.

Concerning the remaining principles of the acts that have to be complied with- such as those concerning safeguards, the obligation to notify and access rights- differences only appear in the respect that under UK law access to information is only provided for the payment of a small fee. Apart from this no material differences occur.

As a conclusion German and UK law do not differ to a recognisable extent in the context of the V-man project. It thus does not make a difference for the laboratory whether German or UK law is applied to the project.

4 Applicable law

Since the laboratory is situated in Glasgow, UK law is applicable.

5 Analysis of the Rights of a person on his/her own image

The V-man project consists of scanning individuals to create and exploit digital clones of these individuals. This section will examine how rights relating to one's image may limit the use that 3D-MATIC can make of them. It will show that European rules relating to performers rights do not apply to the V-man project (1.)). It will then describe the laws of several European countries, underlining that the laws dealing with privacy, publicity and personality still remain largely jurisdiction specific, and focusing on the laws applicable in the UK (2.)). Issues arising as to jurisdiction and applicable law will then be examined (3.)) before drawing a conclusion (4.)).

5.1 European Law and performers' rights

There are no general rules to protect the rights of a person on his/her image at the European level. However, there are specific rules as to performers' rights. Directive 2001/29 EC on the harmonisation of certain aspects of copyright and related rights in the information society which came into force on December 22, 2002 provides that:

> *Member States shall provide for the exclusive right to authorise or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part:*
> *[…]*
> *(b) for performers, of fixations of their performances;*

Article 3 on the right of communication to the public of works and right of making available to the public other subject-matter provides that:

> *[…]*
> *2. Member States shall provide for the exclusive right to authorise or prohibit the making available to the public, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them: (a) for performers, of fixations of their performances;*

The Rome International Convention For The Protection Of Performers, Producers Of Phonograms And Broadcasting Organisations of 1961, to which the UK is a party provides in its 3rd article that:

> *For the purposes of this Convention:*
> *(a) "performers" means actors, singers, musicians, dancers, and other persons who act, sing, deliver, declaim, play in, or otherwise perform literary or artistic works;*

These rules are implemented in British law by the Copyright, Designs and patents Act 1988. Section 180(1)(a) of this act requires the performer to consent to the exploitation of his/her performances. Even though the word "performer" is not defined by the act, a performer would be anyone giving a performance falling under one of the listed categories of performances in section 180(2) :

> *performance" means--*
> *(a) a dramatic performance (which includes dance and mime),*

(b) a musical performance,

(c) a reading or recitation of a literary work, or

(d) a performance of a variety act or any similar presentation,

which is, or so far as it is, a live performance given by one or more individuals;

It appears that models, which are doing none of the above, are excluded from this definition and therefore unable to benefit from transmitting economic rights in their image.

5.2 Image rights under the domestic laws of European countries

5.2.1 UK

Scotland has no specific rule as to image rights. Hence, the rules of English law will be applicable. In English law, a person has no right to his/her voice or image[40]. Therefore, in Great Britain, one cannot prevent the unauthorised use of his/her/her likeness as such. However, the agent making use of the likeness must follow certain rules in order not to breach the model's rights. These are the laws of Passing Off (aa.), defamation (bb.) and restraint of trade (cc.).

5.2.1.1 Passing off

Passing off is '(1) a misrepresentation (2) made by a trader in the course of trade (3) to prospective customers of his or ultimate consumers of goods supplied by him, (4) which is calculated to injure the business or goodwill of another trader (in the sense that it is a reasonably foreseeable consequence) and (5) which causes actual damage to a business or goodwill of the trader by whom the action is brought or, in a quia timet action will probably do so.'[41]

This would apply where a misrepresentation made by 3D-MATIC would be such as to damage its model's goodwill. It would require (a) the model to have goodwill, (b) that 3D-MATIC made a misrepresentation and (c) that this misrepresentation damaged the model's goodwill.

5.2.1.1.1 Goodwill

Goodwill is "The benefit and advantage of the good name, reputation and connection of a business. It is the attractive force which brings in custom"[42] Hence, for a model to establish that s/he has goodwill, s/he must

[40] Cornish, *Intellectual Property* ed.) 16-34; *Erven Warnink Besloten Vennootschap v. J. Townend & Sons (Hull) Ltd* [1979] A.C. 731 at 742, per Lord Diplock; Lord Macnaghten in *IRC v Muler & Co.'s Margarine Ltd* [1901] A.C.217 at 223-4. (4th ed.) 16-34.
[41] *Erven Warnink Besloten Vennootschap v. J. Townend & Sons (Hull) Ltd* [1979] A.C. 731 at 742, per Lord Diplock.
[42] Lord Macnaghten in *IRC v Muler & Co.'s Margarine Ltd* [1901] A.C.217 at 223-4.

establish that s/he is in some sense carrying on a business, and that the public associates his/her/her likeness to this business. It is therefore necessary to be a celebrity.

Recent case law suggests that a model can have a business in his/her likeness (actors, professional models, sportsmen etc…) as to product endorsement[43].

5.2.1.1.2 Misrepresentation

The plaintiff "must demonstrate a misrepresentation by the defendant to the public (whether or not intentional) leading or likely to lead the public to believe that the goods or services offered are of the plaintiff"[44]. There must be some kind of confusion. In deciding whether confusion is likely to result, the test is whether a substantial number of ordinary sensible members of the public would be misled into purchasing the defendant's product in the belief that it was the plaintiff's[45]

This would be the case for product endorsement, where the celebrity "tells the relevant public that he approves of the product or service or is happy to be associated with it. In effect he adds his name as an encouragement to members of the relevant public to buy or use the service or product"[46]. But product endorsement is to be distinguished from merchandising which consists of exploiting an image, which has become famous, the exploitation being made whether or not approved of or consented to by the celebrity[47].

As to the current state of case law, misrepresentation can lie in false endorsement (ie: unlicensed endorsement) but no in merchandising. Nevertheless, the division between endorsement and merchandising is unclear and they often overlap. Moreover, courts tend to extend the legal field to which passing off applies. It is therefore better, for legal safety, to always have a consent from the celebrity to use his/her image.

5.2.1.1.3 Damage

Here, the plaintiff must show that s/he suffers or is likely to suffer damage by reason of the erroneous belief engendered by the defendant's misrepresentation. This can be the case if s/he shows that s/he will lose royalties or that s/he will lose control over the quality of the goods on which the name, character or likeness is reproduced[48].

5.2.1.1.4 Summary

[43] *Irvine v Talksport Ltd* [2002] EWHC 367; [2002] 2 All E.R. 414 (Ch D), confirmed by *Irvine v Talksport*, [2003] ECWA Civ 423 1/04/2003.
[44] *Reckitt & Colman Properties Ltd v. Borden Inc*. [1990] 1 W.L.R. 491 at 499, HL.
[45] Vincent Nelson, *The law of entertainment and Broadcasting* (Second edition) Sweet and Maxwell, 289.
[46] Laddie J in *Irvine v Talksport Ltd* [2002].
[47] Alexander Learmonth, 'Eddie, Are You Okay? Product Endorsement And Passing Off', [2002] 3 IPQ, 307.
[48] Vincent Nelson, *The law of entertainment*, 293.

For an action in passing off to succeed, the model would have to prove:

1. Goodwill: That s/he is a celebrity and that s/he has engaged in a business over his/her likeness
2. Misrepresentation: That 3D-MATIC has used his/her likeness without prior consent to endorse a product
3. Damage: that has suffered or is likely to suffer from a loss of royalties.

5.2.1.2 Defamation

"The tort of defamation consists in the publication to a person other than the plaintiff of a statement of and concerning the plaintiff, where such statement is untrue in substance and in fact, and is defamatory in nature."[49]

3D-MATIC must therefore ensure that it does not use the model's images in any way that would be insulting or defamatory to the model, or which would lead the public to believe something that is untrue as to the model.

5.2.1.3 Restraint of trade

All interference with the individual's liberty of action in trading, and all restraints of trade themselves if there is nothing more, is contrary to public policy and therefore prima facie void[50]. This would apply where a restraint imposed by 3D-MATIC on the model would be unreasonable and would offend against public policy.

5.2.1.3.1 What is a restraint?

A restraint is "… Any contract which interferes with the free exercise of his trade or business, by restricting… the work he may do for other".[51] More precisely, as described in another case, "If an artist is effectively able to be prevented from reaching to the public over a prolonged period I find it unrealistic to say that this is not a contract in restraint"[52]

Hence, there would be a restraint if 3D-MATIC forbade a model from using his/her likeness for any period of time.

5.2.1.3.2 When is a restraint unreasonable or offending against public policy?

To determine reasonableness it is necessary to identify the interest that the party imposing the restraint is trying to protect. That interest has to be legitimate.[53] However, what were the legitimate interests and whether the restraint is reasonable are both questions of fact, to be decided on a case-by-case basis.

---

[49] Vincent Nelson, *The law of entertainment*, 327.
[50] *Nordenfelt v. Maxim Nordenfelt Guns & Ammunition Co. Ltd* [1894] A.C. 535, HL.
[51] Lord Denning M.R. in *Petrofina (Great Britain) Ltd v. Martin* [1966] Ch. 169.
[52] *Silverstone Records v. Mountfield* [1993] E.M.L.R. 160.
[53] Vincent Nelson, *The law of entertainment*, 45.

As a general guidance, "The duration of an agreement in restraint of trade is a factor of great importance in determining whether the restrictions in the agreement can be justified"[54] Moreover, where the economic strength of the parties is unbalanced, a restraint is more likely to be held unreasonable.

Further, as to public policy, "The public interest requires in the interests both of the public and of the individual that everyone should be free so far as practicable to earn a livelihood and to give to the public the fruits of his particular abilities. The main question to be considered is whether and how far the operation of the terms of this agreement is likely to conflict with this objective."[55]

Hence, if 3D-MATIC wishes to place a restraint on the models to prevent them from consenting to the use of their image by other corporations, it is important to do it on a case by case basis. 3D-MATIC must be seeking to protect a legitimate interest, such as protecting the uniqueness of a product. It is the likeness of the model, which must constitute the uniqueness of the product. Moreover, the restraint must be limited in scope and in time.

5.2.1.3.3 Conclusion

It is not advised to place such a restraint in a model consent. However, such a restraint could be placed in specific consents with specific models, where 3D-MATIC believes it is in its interest to have a monopoly over the model's likeness and where it ensures that such a restraint does not prevent the model from earning a livelihood from its likeness. Such a restraint would have to be limited in scope and in time.

5.2.2 France

Derived from article 9 of the Code civil, French courts have recognised, as a general principle of law that every person benefits from the exclusive right to forbid the reproduction or the use of his/her image without his/her explicit and specific authorisation[56]. It is thus necessary to obtain the consent of a person before using his/her image.

The authorisation must be specific. For instance, where a model has consented to the use of her image on a web site, this consent does not amount to an authorisation to animate this image on the web site[57]. Hence, the consent must specify every intended use and every intended mean of exploitation. The consent given by a person to capture, publish and exploit his/her image can only be given for a limited duration[58].

5.2.3 Sweden

[54] Lord Reid in *A. Schroeder Publishing v. Macaulay* [1974] 1 W.L.R. 1308 HL.
[55] Lord Reid in *A. Schroeder Publishing v. Macaulay* [1974] 1 W.L.R. 1313 HL.
[56] TGI Paris, 27/01/1997.
[57] TGI Paris, 5/01/2000.
[58] Paris, 10/11/1988.

In Sweden consent must be obtained to use the name or photograph of an individual for the marketing of a product. Use without consent may give rise to a claim for damages.

5.2.4 Spain

Spain protects the privacy of its citizens by way of constitutional rights. The rights of reputation, privacy and image are recognised in Article 18(1) of the 1978 Spanish Constitution. Another limit to what the producer can do comes from the Act 1/1982 for the protection of reputation, privacy and image.

5.2.5 Ireland

Ireland protects the privacy of its citizens by way of constitutional rights. The Irish Courts have recognised an unenumerated constitutional right to privacy.

5.2.6 Netherlands

Netherlands protects personality rights by copyright and privacy legislation, and specifically protects portrait rights by statute.

5.2.7 Belgium

Belgium recognises "*image rights*", the Belgian Courts awarding damages for breach.

5.2.8 Germany

Germany has enacted express copyright provisions to the protection of one's own image or personal portrayal. A person has the exclusive right to decide whether a photograph of her or her image may be used for publication or not. Some exceptions are made for "*persons of contemporary history*" such as politicians, actors and sportsmen who must tolerate their photographs being published without consent unless the reproduction is in the form of an "inadequate or disgusting" context.

5.3 Jurisdiction

In all European countries, the laws relating to image rights are part of tort law. Two issues arise. Which is the jurisdiction (i.e.: the courts from which country?) competent to deal with a legal dispute over image rights and which law will apply? Both issues will only arise where there is a foreign element involved. This occurs when the elements relating to the dispute are divided between different countries, for example when the parties have

different nationalities or when any element takes place in a country different from that of the parties' nationality. If all the elements are linked to only one country, the courts of that country will have jurisdiction, and the laws of that country will be applicable. If there is at least one foreign element, two sets of rule apply for jurisdiction matters (a.)) and applicable law matters (b.)).

5.3.1 Regulation (EC) No 44/2001

Jurisdiction is dealt with by Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. This regulation applies to all countries of the European Union. Article 2 of the regulation sets a general rule: *persons domiciled in a Member State shall, whatever their nationality, be sued in the courts of that Member State*. Hence, if 3D-MATIC were to be sued by a model, the plaintiff would have to sue before Scottish courts.

However, article 5(3) of the regulation sets a rule of special jurisdiction in matters relating to torts.

> *Article 5*
> *A person domiciled in a Member State may, in another Member State, be sued:*
>
> *[…]*
>
> *3. in matters relating to tort, delict or quasi-delict, in the courts for the place where the harmful event occurred or may occur;*

Following this rule of special jurisdiction, 3D-MATIC could be sued before the courts of any country where the images of the scanned models are distributed. To avoid this, and to make sure that the Scottish courts will always have jurisdiction, it is possible to include a jurisdiction clause in the consent signed by the models. This jurisdiction clause will specify that exclusive jurisdiction should be granted to the courts of Scotland in the event of any dispute over the consent.

For the jurisdiction clause to be valid, at least one of the parties must be domiciled in a Member State (art 23). It must be in writing (art 23(a)) and contained in a document signed by both parties[59].

5.3.2 Applicable law

The issue of applicable law is dealt with by EC Convention on the Law Applicable to Contractual Obligations (Rome 1980), implemented in English law by the Contracts (Applicable law) Act 1990. The principle is that the parties are free to choose the law the law applicable to their contract (art 3.1) in any situation involving a choice between the laws of different countries (art 1(1)). For the choice of applicable law to be valid, it must be expressed or demonstrated with reasonable certainty by the terms of the contract (art 3.1).

[59] ECJ *Tilly Russ v. Nova* 1984.

5.3.2.1 Material validity of the applicable law clause

This relates to the formation of the contract. Art 8(1) provides that the existence and validity of a contract is to be determined by the law, which would govern it under the Convention if the contract or term were valid. Hence, where the party have chosen a law to govern the contract, the existence and validity of the contract is to be determined by that law. As a consequence, where Scottish law is chosen, the existence and validity of the consent is to be determined under Scottish law.

5.3.2.2 Formal validity of the applicable law clause

This relates to the form of the contract. Under art 9(1), where parties are in the same country, the contract will be valid if it meets the requirement of either the governing law (the law that governs the contract, as chosen by the parties) or of the law of the country where it is concluded. Hence, if both parties are in Italy, and the contract if governed by Scottish law, the contract is formally valid if it satisfies the requirements of either Scottish or Italian law.

Under art 9(2), where parties are in different countries, the contract will be valid if it meets the requirement of either the governing law or of the laws of either of the countries where the parties are present.

As 3D-MATIC is located in Scotland, Scottish law can be chosen as the governing law of the consent. The effect of the jurisdiction clause will be to give exclusive jurisdiction to the Scottish courts. The effect of the applicable law clause will be to have the consent governed by Scottish law.

6 Conclusion

From the above analysis, it appears that 3D-MATIC would benefit from conferring exclusive jurisdiction to Scottish courts and from choosing Scottish law to govern the contracts signed with its models. Two arguments justify this choice. First, where there is no foreign element, Scottish courts will automatically have jurisdiction and Scottish law will automatically apply. This will be the case where the model is Scottish and the dispute concerns the use of his/her images in Scotland.

Second, where there is a foreign element, 3D-MATIC will expose lower legal fees where the dispute is dealt with by Scottish courts. Moreover, the laws relating to image rights in Scotland are much more protective of 3D-MATIC's rights than the laws of other European countries.

By choosing Scottish law as the governing law of the contracts signed with the models, 3D-MATIC will have to ensure that it is not using the images in any way that would be insulting or defamatory to the model, or which would lead the public to believe something that is untrue as to the model. 3D-MATIC will also have to ensure that it is not acting in restraint of trade toward the model, unless such a restraint has been specifically negotiated and is not unreasonable.

Appendix 1: Model Consent

The model:

First name:
Surname:
Address:
Post Code:
City:
Country:

The Controllers of personal information:

Any personal information will be processed and controlled by:
3D-MATIC
Boyd Orr Building, Room 417
University of Glasgow
University Avenue
Glasgow G12 8QQ
United Kingdom

Consent to data processing:

1. The model agrees to 3D-MATIC taking, reproducing and releasing to the public pictures and scans of the model. The model agrees to 3D-MATIC processing these pictures and scans by computerised means in existence or yet to be invented, to obtain a fully animated and photo-realistic 3 dimensional digital character, using the model's likeness. The model agrees to 3D-MATIC reproducing and releasing this 3 dimensional digital character to the public.

2. The pictures, scans and 3 dimensional digital character (hereinafter "the images") can be exploited directly by 3D-MATIC, or transferred to third parties for such exploitation, in whole or in part, by all means and in all media in existence or yet to be invented, worldwide, free of any restrictions, including, but not limited to:

- For the film industry, or any mean of production in existence or yet to be invented of audiovisual works;
- For the software industry, including, but not limited to, computer animation, film and video post-production, virtual actors, computer games, crowd simulations, clothing sizing, vehicle design and workspace design;
- For the alteration or modification of the images, including, but not limited to, morphing or alteration or modification of the physical appearance of the model;

- For the showing to paying and non-paying audience;
- For the showing on television or pay television, including, but not limited to, by broadcasting, cable, satellite or any other form of television distribution in existence or yet to be invented;
- For use on the internet, including, but not limited to, on websites;
- For use in commercial advertisements, including, but not limited to, on television, radio, internet, theatres, in printed or edited form or any other mean or media in existence or yet to be invented;
- For promotional and/or demonstration purposes;
- For exploitation of the images on any media in existence or yet to be invented including but not limited to videodiscs, videocassettes or slides;
- For electronic editing, including, but not limited to, CD-Rom, CD-I, DVD or any other mean in existence or yet to be invented.
- For the reproduction of the images in any kind of printed or edited form, including, but not limited to, journals, newspapers, periodicals, magazines, books, postcards, posters, catalogues, agendas or games;
- For the reproduction of the images on garments, curio or any merchandising mean in existence or yet to be invented;
- For the usage of the images for an unlimited period of time.

3. The model is aware and agrees to the processing of his sensitive data (such as race) for the above purposes, since the images will reveal his physical appearance in great detail.

4. The model agrees to voices being used in association with his images for dubbing purposes.

5. The model agrees to 3D-MATIC transferring the images to third parties located outside the European Union.

6. The model guarantees that s/he is not bound by any exclusive agreement as to the exploitation of his/her likeness.

7. 3D-MATIC will expressly refrain from exploiting the images in any way likely to damage the model's reputation. In particular, 3D-MATIC will not use the material in any kind of pornographic, racist or xenophobe work.

8. 3D-MATIC will, at regular intervals and if the model so requests, put its best efforts in providing the model with accurate information as to how and for which purpose the images are being used and to whom they have been disclosed. 3D-MATIC will also put its best efforts in encouraging its business partners to do the same.

9. The model confirms that he is of full age (18 years) otherwise the validity of the contract is dependent on the consent of the legal representative.

Fees:

In consideration for the model's obligations, 3D-MATIC agrees to pay to the model a fee of. ……£

Choice of law and Jurisdiction:

This agreement shall be construed under and governed by the laws of Scotland and the parties agree to submit to the exclusive jurisdiction of the Scottish courts.

Done at Glasgow,

2 copies of this contract were issued, one of them remaining with the model.

Date:……..

……	.....
The model	Representing 3D-MATIC

Appendix 2: Illustrative list of safeguards to be ensured

Some of the security controls that the data controller is likely to need to consider are set out below. (This is not a comprehensive list but is illustrative only.)
Security management:

- does the data controller have a security policy setting out management commitment to information security within the organisation?

- is responsibility for the organisation's security policy clearly placed on a particular person or department?

- are sufficient resources and facilities made available to enable that responsibility to be fulfilled?

Controlling access to information:

- is access to the building or room controlled or can anybody walk in?

- can casual passers-by read information off screens or documents?

- are passwords known only to authorised people and are the passwords changed regularly?

- do passwords give access to all levels of the system or only to those personal data with which that employee should be concerned?

- is there a procedure for cleaning media (such as tapes and disks) before they are reused or are new data merely written over old? In the latter case is there a possibility of the old data reaching somebody who is not authorised to receive it? (e.g. as a result of the disposal of redundant equipment).

- is printed material disposed of securely, for example, by shredding?

- is there a procedure for authenticating the identity of a person to whom personal data may be disclosed over the telephone prior to the disclosure of the personal data?

- is there a procedure covering the temporary removal of personal data from the data controller's premises, for example, for staff to work on at home? What security measures are individual members of staff required to take in such circumstances?

- are responsibilities for security clearly defined between a data processor and its customers?

Ensuring business continuity:

- are the precautions against burglary, fire or natural disaster adequate?

- is the system capable of checking that the data are valid and initiating the production of back-up copies? If so, is full use made of these facilities?

- are back-up copies of all the data stored separately from the live files?

- is there protection against corruption by viruses or other forms of intrusion?

Staff selection and training:

- is proper weight given to the discretion and integrity of staff when they are being considered for employment or promotion or for a move to an area where they will have access to personal data?

- are the staff aware of their responsibilities? Have they been given adequate training and is their knowledge kept up to date?

- do disciplinary rules and procedures take account of the requirements of the Act? Are these rules enforced?

- does an employee found to be unreliable have his or her access to personal data withdrawn immediately?

- are staff made aware that data should only be accessed for business purposes and not for their own private purposes?

  Detecting and dealing with breaches of security:

  - do systems keep audit trails so that access to personal data is logged and can be attributed to a particular person?

  - are breaches of security properly investigated and remedied; particularly when damage or distress could be caused to an individual?

  The Act introduces express obligations upon data controllers when the processing of personal data is carried out by a data processor on behalf of the data controller. In order to comply with the Seventh Principle the data controller must –

- choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures they take,

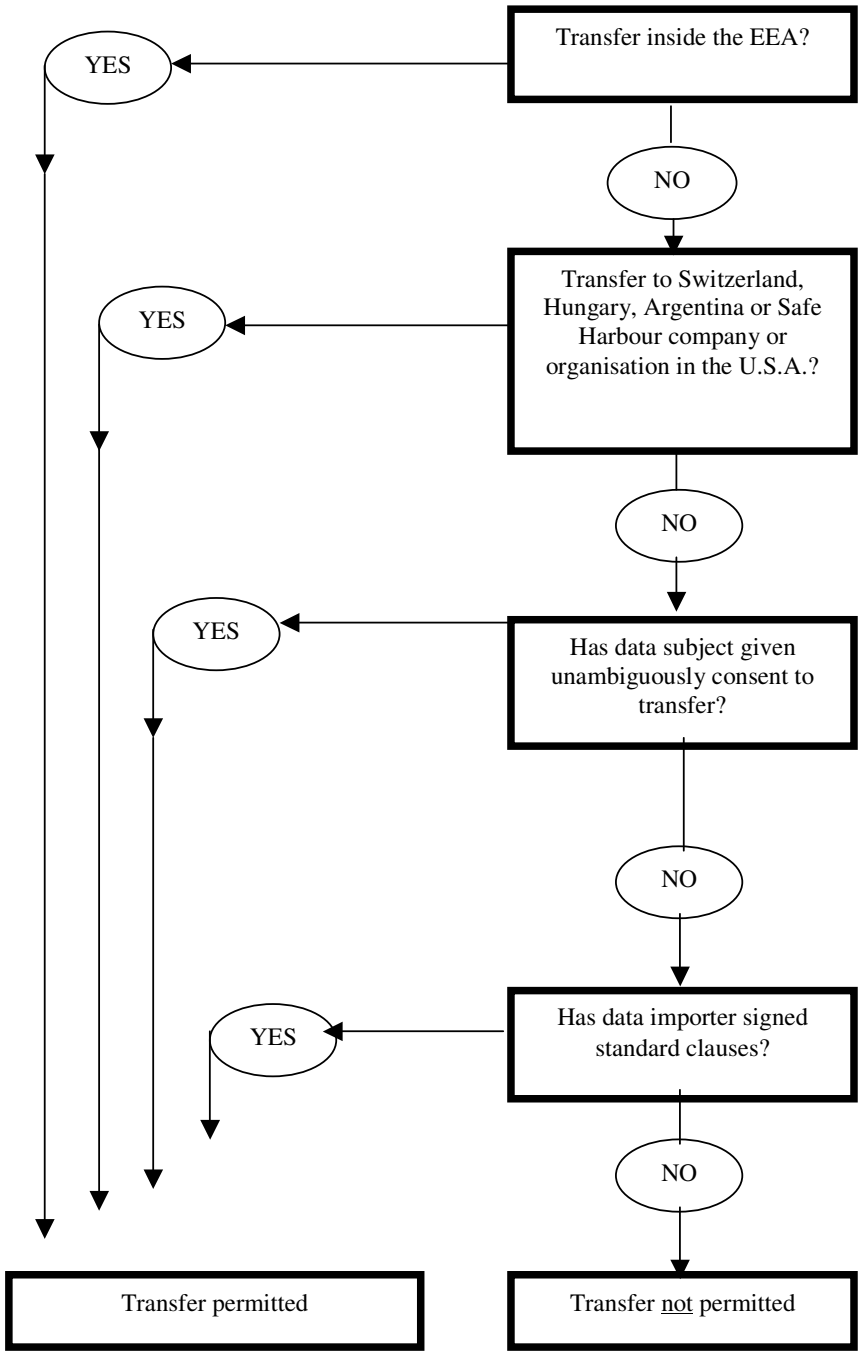
- take reasonable steps to ensure compliance with those measures, and

- ensure that the processing by the data processor is carried out under a contract, which is made or evidenced in writing, under which the data processor is to act only on instructions from the data controller. The contract must require the data processor to comply with obligations equivalent to those imposed on the data controller by the Seventh Principle.

  Further advice may be found in BS 7799 and 1S0/IEC Standard 17799.

It is important to note that the Seventh Principle relates to the security of the processing as a whole and the measures to be taken by data controllers to provide security against any breaches of the Act rather than just breaches of security.

Appendix 3: Transborder data flow checklist



Appendix 4: Standard Clauses for transfer to third countries

ANNEX

STANDARD CONTRACTUAL CLAUSES

for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to third countries which do not ensure an adequate level of protection

Name of the data exporting organisation: .....

.....

Address: .....

Tel. ..... **fax** ..... **e-mail:** .....

Other information needed to identify the organisation: .....

('the data **exporter**')

and

Name of the data importing organisation: .....

.....

Address: .....

tel. ..... **fax** ..... **e-mail:** .....

Other information needed to identify the organisation: .....

('the data **importer**')

HAVE AGREED on the following contractual clauses ('the Clauses') in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1:

Clause 1

Definitions

For the purposes of the Clauses:

a) '**personal data**', '**special categories of data**', '**process/processing**', '**controller**', '**processor**', '**data subject**' and '**supervisory authority**' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('hereinafter the Directive');

b) the '**data exporter**' shall mean the controller who transfers the personal data;

c) the '**data importer**' shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection.

Clause 2

Details of the transfer

The details of the transfer, and in particular the categories of personal data and the purposes for which they are transferred, are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

The data subjects can enforce this Clause, Clause 4(b), (c) and (d), Clause 5(a), (b), (c) and (e), Clause 6(1) and (2), and Clauses 7, 9 and 11 as third-party beneficiaries. The parties do not object to the data subjects being represented by an association or other bodies if they so wish and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data by him has been and, up to the moment of the transfer, will continue to be carried out in accordance with the relevant provisions of the Member State in which the data exporter is established (and where applicable has been notified to the relevant authorities of that State) and does not violate the relevant provisions of that State;

(b) that if the transfer involves special categories of data the data subject has been informed or will be informed before the transfer that this data could be transmitted to a third country not providing adequate protection;

(c) to make available to the data subjects upon request a copy of the Clauses; and

(d) to respond in a reasonable time and to the extent reasonably possible to enquries from the supervisory authority on the processing of the relevant personal data by the data importer and to any enquiries from the data subject concerning the processing of this personal data by the data importer.

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) that he has no reason to believe that the legislation applicable to him prevents him from fulfilling his obligations under the contract and that in the event of a change in that legislation which is likely to have a substantial adverse effect on the guarantees provided by the Clauses, he will notify the change to the data exporter and to the supervisory authority where the data exporter is established, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) to process the personal data in accordance with the mandatory data protection principles set out in Appendix 2;
or, if explicitly agreed by the parties by ticking below and subject to compliance with the mandatory data protection principles set out in Appendix 3, to process in all other respects the data in accordance with:

— the relevant provisions of national law (attached to these Clauses) protecting the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data applicable to a data controller in the country in which the data exporter is established, or

— the relevant provisions of any Commission Decision under Article 25(6) of Directive 95/46/EC finding that a third country provides adequate protection in certain sectors of activity only, if the data importer is based in that third country and is not covered by those provisions, in so far as those provisions are of a nature which makes them applicable in the sector of the transfer;

(c) to deal promptly and properly with all reasonable inquiries from the data exporter or the data subject relating to his processing of the personal data subject to the transfer and to cooperate with the competent supervisory authority in the course of all its inquries and abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(d) at the request of the data exporter to submit its data processing facilities for audit which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(e) to make available to the data subject upon request a copy of the Clauses and indicate the office which handles complaints.

Clause 6

Liability

1. The parties agree that a data subject who has suffered damage as a result of any violation of the provisions referred to in Clause 3 is entitled to receive compensation from the parties for the damage suffered. The parties agree that they may be exempted from this liability only if they prove that neither of them is responsible for the violation of those provisions.

2. The data exporter and the data importer agree that they will be jointly and severally liable for damage to the data subject resulting from any violation referred to in paragraph 1. In the event of such a violation, the data exporter or the data importer or both.

3. The parties agree that if one party is held liable for a violation referred to in paragraph 1 by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred. (*).

Clause 7

Mediation and jurisdiction

1. The parties agree that if there is a dispute between a data subject and either party which is not amicably resolved and the data subject invokes the third-party beneficiary provision in clause 3, they accept the decision of the data subject:

(a) to refer the dispute to mediation by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that by agreement between a data subject and the relevant party a dispute can be referred to an arbitration body, if that party is established in a country which has ratified the New York convention on enforcement of arbitration awards.

3. The parties agree that paragraphs 1 and 2 apply without prejudice to the data subject's substantitve or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

The parties agree to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under national law.

Clause 9

Termination of the Clauses

The parties agree that the termination of the Clauses at any time, in any circumstances and for whatever reason does not exempt them from the obligations and/or conditions under the Clauses as regards the processing of the data transferred.

Clause 10

Governing Law

The Clauses shall be governed by the law of the Member State in which the Data Exporter is established, namely .....

.....

Clause 11

Variation of the contract

The parties undertake not to vary or modify the terms of the clauses.

On behalf of the data exporter:

Name (written out in full): .....

Position: .....

Address: .....

Other information necessary in order for the contract to be binding (if any): .....

.....

.....
(signature)

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): .....

Position: .....

Address: .....

Other information necessary in order for the contract to be binding (if any): .....

.....

.....

.....
(signature)

(stamp of organisation)

Appendix 1

to the standard contractual clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

(The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.)

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

.....

.....

.....

Data importer

The data importer is (please specify briefly your activities relevant to the transfer):

.....

.....

.....

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

.....

.....

.....

Purposes of the transfer

The transfer is necessary for the following purposes (please specify):

.....

.....

.....

Categories of data

The personal data transferred fall within the following categories of data (please specify):

.....

.....

.....

Sensitive data (if appropriate)

The personal data transferred fall within the following categories of sensitive data (please specify):

.....

.....

.....

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients (please specify):

.....

.....

.....

Storage limit

The personal data transferred may be stored for no more than (please indicate): ..... (months/years)

Data exporter	Data importer
Name:	Name: .....
..... (Authorised signature)	..... (Authorised signature)

Appendix 2

to the standard contractual clauses

Mandatory data protection principles referred to in the first paragraph of Clause 5(b)

These data protection principles should be read and interpreted in the light of the provisions (principles and relevant exceptions) of Directive 95/46/EC.

They shall apply subject to the mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others.

1. *Purpose limitation*: data must be processed and subsequently used or further communicated only for the specific purposes in Appendix I to the Clauses. Data must not be kept longer than necessary for the purposes for which they are transferred.

2. *Data quality and proportionality*: data must be accurate and, where necessary, kept up to date. The data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. *Transparency*: data subjects must be provided with information as to the purposes of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fair processing, unless such information has already been given by the data exporter.

4. *Security and confidentiality*: technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as unauthorised access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the controller.

5. *Rights of access, rectification, erasure and blocking of data*: as provided for in Article 12 of Directive 95/46/EC, the data subject must have a right of access to all data relating to him that are processed and, as appropriate, the right to the rectification, erasure or blocking of data the processing of which does not comply with the principles set out in this Appendix, in particular because the data are incomplete or inaccurate. He should also be able to object to the processing of the data relating to him on compelling legitimate grounds relating to his particular situation.

6. *Restrictions on onwards transfers*: further transfers of personal data from the data importer to another controller established in a third country not providing adequate protection or not covered by a decision adopted by the Commission pursuant to Article 25(6) of Directive 95/46/EC (onward transfer) may take place only if either:

   (a) data subjects have, in the case of special categories of data, given their unambiguous consent to the onward transfer or, in other cases, have been given the opportunity to object.

   The minimum information to be provided to data subjects must contain in a language understandable to them:

   — the purposes of the onward transfer,

   — the identification of the data exporter established in the Community,

   — the categories of further recipients of the data and the countries of destination, and

   — an explanation that, after the onward transfer, the data may be processed by a controller established in a country where there is not an adequate level of protection of the privacy of individuals; or

   (b) the data exporter and the data importer agree to the adherence to the Clauses of another controller which thereby becomes a party to the Clauses and assumes the same obligations as the data importer.

7. *Special categories of data*: where data revealing racial or ehtnic origin, political opinions, religious or philosophical beliefs or trade union memberships and data concerning health or sex life and data relating to offences, criminal convictions or security measures are processed, additional safeguards should be in place within the meaning of Directive 95/46/EC, in particular, appropriate security measures such as strong encryption for transmission or such as keeping a record of access to sensitive data.

8. *Direct marketing*: where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to 'opt-out' from having his data used for such purposes.

9. *Automated individual decisions*: data subjects are entitled not to be subject to a decision which is based soley on automated processing of data, unless other measures are taken to safeguard the individual's legitimate interests as provided for in Article 15(2) of Directive 95/46/EC. Where the purpose of the transfer is the taking of an automated decision as referred to in Article 15 of Directive 95/46/EC, which produces legal effects concerning the individual 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., the individual should have the right to know the reasoning for this decision.

Appendix 3

to the standard contractual clauses

Mandatory data protection principles referred to in the second paragraph of Clause 5(b)

1. *Purpose limitation*: data must be processed and subsequently used or further communicated only for the specific purposes in Appendix I to the Clauses. Data must not be kept longer than necessary for the purposes for which they are transferred.

2. *Rights of access, rectification, erasure and blocking of data*: as provided for in Article 12 of Directive 95/46/EC, the data subject must have a right of access to all data relating to him that are processed and, as appropriate, the right to the rectification, erasure or blocking of data the processing of which does not comply with the principles set out in this Appendix, in particular because the data is incomplete or inaccurate. He should also be able to object to the processing of the data relating to him on compelling legitimate grounds relating to his particular situation.

3. *Restrictions on onward transfers*: further transfers of personal data from the data importer to another controller established in a third country not providing adequate protection or not covered by a decision adopted by the Commission pursuant to Article 25(6) of Directive 95/46/EC (onward transfer) may take place only if either:

   (a) data subjects have, in the case of special categories of data, given their unambiguous consent to the onward transfer, or, in other cases, have been given the opportunity to object.

   The minimum information to be provided to data subjects must contain in a language understandable to them:
   — the purposes of the onward transfer,
   — the identification of the data exporter established in the Community,
   — the categories of further recipients of the data and the countries of destination, and
   — an explanation that, after the onward transfer, the data may be processed by a controller established in a country where there is not an adequate level of protection of the privacy of indidividuals; or

   (b) the data exporter and the data importer agree to the adherence to the Clauses of another controller which thereby becomes a party to the Clauses and assumes the same obligations as the data importer.
