BEST PRACTICE GUIDE

EUROPEAN GENERAL DATA PROTECTION REGULATION
CONSEQUENCES FOR DIALOGUE MARKETING

Compliance
Transparency
Service Provider
Implementation
Cross-border
Processing

DDV
Deutscher
Dialogmarketing
Verband e.V.

Publisher
Deutscher Dialogmarketing Verband e.V.
Hahnstraße 70
D-60528 Frankfurt/Main
Tel. +49 69 401 276 500
Fax +49 69 401 276 599
eMail: info@ddv.de
www.ddv.de

Design
rahlwespietz, Frankfurt/Main

Published
August 2016

CONTENT

INTRODUCTION

On 25 May 2018, the General European Data Protection Regulation (2016/679/EU) (the "**Regulation**") will largely replace the current national data protection laws in the European Union. The Regulation will harmonise the data protection rules essential to dialogue marketing across Europe. Member States will have limited freedom to apply deviating national requirements. This Best Practice Guide outlines the application of the Regulation in the daily operations of dialogue marketing.

One of the central data protection questions in dialogue marketing is whether personal data can be processed for marketing purposes without the consent of the data subject. The European legislator has decided to retain the so-called Opt-out Principle, under which the data subject has the right to object to the use of his or her personal data for dialogue marketing purposes without giving any reasons and at any time. In this way, the Regulation reconciles the right of data subjects to self-determination with the economic goals of the European Union.

The Opt-out Principle, however, does not apply without limitations. The legitimate interests of the data subjects must be adequately taken into account. Sufficient transparency regarding the use of the data must also be established. The Directive on privacy and electronic communications (2002/58/EC) (the "**ePrivacy Directive**"), and the national laws implementing it, place additional restrictions on electronic advertising communication. The ePrivacy Directive is being reviewed by the European Commission and may be reformed as early as the summer of 2018. However, the form and the contents of any such new rules is still under discussion.

As compared to the existing national data protection laws, the Regulation contains a number of innovations. Overall, the Regulation does not reduce the level of protection for personal data. It will replace certain detailed national provisions by more general provisions. The use of data for marketing purposes will be subject to a general balance-of-interests test. The transparency requirements and the rights of data subjects will increase. The data protection supervisory authorities will be granted more far-reaching rights to intervene and to impose sanctions.

However, the Regulation leaves reasonable flexibility for dialogue marketing activities. The main challenges arise in the interpretation of the new provisions in detail, because the lengthy negotiations in Brussels and Strasbourg failed to produce clear and consistent Arti-

cles and Recitals. The Best Practice Guide aims to develop practical solutions for complying with the Regulation, taking into account its general goals.

This Best Practice Guide provides a preliminary assessment of compliance with the Regulation. Details of the data protection regime – such as the national implementing provisions and the ePrivacy Directive – will continue to develop until 25 May 2018, when the Regulation becomes applicable. The German Dialogue Marketing Association (*Deutscher Dialogmarketing Verband e.V. – "**DDV"***) will actively monitor this process and this Best Practice Guide will be amended accordingly at the appropriate time.

The provisions of the Regulation have been drafted in fairly general terms and will likely lead to diverging interpretations. Member States may tend to interpret the rules in such a way as to conform to their existing specific national provisions. This will create inconsistencies, and generally contradict the Regulation's general goal of harmonising data protection laws across Europe. For such reasons, this Best Practice Guide intentionally does not take into account specific existing national laws when interpreting the Regulation.

Companies cannot afford to ignore the Regulation until it becomes applicable and need to begin preparing for the changes that will be introduced by the Regulation. For example, redrafting consent declarations may be required to comply with the Regulation. If such declarations do not meet the requirements of the Regulation as of 25 May 2018, they might become invalid. The extended transparency requirements have to be implemented in time. Agreements for processing by service providers must be aligned with the requirements of the Regulation. Companies must also ensure that their internal procedures comply with the Regulation's requirements by 25 May 2018. This Best Practice Guide provides support to companies as they make such necessary changes.

This Best Practice Guide was authored by the data protection working group of the DDV. Ulrich Wuermeling, Latham & Watkins LLP, Frankfurt, has supported the data protection working group of the DDV as a specialist for many years and has played a significant role in the compilation of this Best Practice Guide. We expressly convey our gratitude to him and the data protection working group of the DDV.

1. DIALOGUE MARKETING IN PRACTICE

1.1 AVAILABLE DATA SOURCES

The aim of dialogue marketing is to communicate with new and existing customers according to their interests. Doing so requires suitable communication channels to the addressees as well as meaningful selection criteria. The communication channels available in dialogue marketing range from advertising by postal mail or electronic mail to Online Behavioural Advertising. Selection criteria are used in order to limit, to the extent possible, the advertising to potentially interested persons. Thus, meaningful selection not only saves money for businesses, but also serves the interests of the addressees.

Companies can employ various data sources to research potential addressees, suitable communication channels and meaningful selection criteria. The most common data sources are prior communications with potential or existing customers and publicly available information. Data can be collected directly from the addressee or made available by other market participants or data service providers. The selection criteria enhance the probability of economically successful dialogue marketing.

Statistical analysis is one method of measuring the effectiveness of selection criteria. The underlying personal data can be condensed into general categories, pseudonymised or anonymized before being used as selection criteria, which helps to protect the data subject's legitimate interests in a manner that is compliant with the Regulation.

1.2 PREPARING AN INDIVIDUAL DIALOGUE

As a first step, an individual dialogue requires a broad pool of potential addressees, including details regarding the available communication channels for reaching them. Such a pool is either collected by the advertiser itself or is provided by other market participants or data service providers.

As a second step, the addressees with a potential interest in the advertised products and services are selected from the pool. Such selection is made on the basis of personal data which might be pseudonymised or anonymised. The advertiser may select the addresses based on the data it has already collected. However, especially where potential new customers are to be contacted, such data will not be sufficient for a meaningful selection. The advertiser may instead or in addition use data provided by other market participants or data service providers. Alternatively, the advertiser might employ procedures under which the

processing of personal data by the advertiser is not required (for example, Lettershops or Online Behavioural Advertising).

The goal of the selection is to compile a group of addressees who potentially share an interest in certain products or services. Once the selection has been made, the selected group is reviewed again in order to improve data quality. The addresses are corrected, updated, and compared against the Robinson list or similar *ad denier* lists. Next, consent might need to be verified for electronic communication. This process eventually yields a list of potentially interested addresses and the suitable communication channels for reaching out to them.

1.3 CONTACTING POTENTIAL CUSTOMERS

Potential customers are contacted via postal or electronic channels. In view of the existing legal barriers regarding communication by e-mail, telephone, telefax or SMS, companies often contact potential customers via postal mail. The communication may be sent directly by the advertiser of the products or services or through other market participants. Online Behavioral Advertising is an exception since addressees are not contacted individually, albeit that advertisements displayed on websites are also tailored to groups of potential customers.

2. CONDUCTING COMPLIANT DIALOGUE MARKETING

2.1 THREE ALTERNATIVES FOR COMPLIANT DIALOGUE MARKETING

Under the Regulation, the processing of personal data requires a legal justification. The processing of personal data for dialogue marketing purposes can be based on three different legal grounds: balance of interests, consent, and compatible purposes. Anonymised data do not constitute personal data and, therefore, the processing of anonymised data does not require legal justification. However, it is not always easy to determine whether data has to be considered anonymous or personal under the Regulation.

§ Personal, pseudonymous or anonymous data?

Generally, dialogue marketing requires personal data, one category of which are pseudonymised data. Data are defined as having been rendered pseudonymous if the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (Article 4(5)).

Selections can also be carried out on the basis of anonymous data. Since the Regulation does not apply to anonymised data, the distinction between personal and anonymised data is of great practical relevance. The processing of anonymised data does not require a legal basis. This is, for example, relevant for so-called micro-geographical data relating to regional segments instead of actual persons.

Personal data are defined as any information relating to an identified or identifiable natural person (Article 4(1)). This definition stems from the European Data Protection Directive. The Regulation contains a number of clarifying examples for instances in which a person might be regarded as identifiable. Identifiers can, for example, consist of identification numbers, location data or online identifiers.

Information is deemed to be personal data if the controller has means at its disposal which “are reasonably likely to be used to identify the natural person” (Recital 26). As long as data are only theoretically identifiable, it cannot be considered to be personal data. If it is not likely that means to identify the data will be used, the data are considered to be anonymous. Similarly, if a third party has the means of identifying a data subject, the data held by the controller will not constitute personal data as long as access to the identifying data is not likely. However, if the third party’s data are reasonably likely to be merged with the data of the controller, the data held will be regarded as personal data.

The distinction between personal and anonymous data can be illustrated using the example of IP addresses and cookies. The Regulation finds that data subjects “may be associated with online identifiers” such as IP addresses or cookies (Recital 30). However, under the Regulation it remains open under what circumstances IP addresses or cookies will make particular data subjects identifiable.

The Court of Justice of the European Union decided that IP addresses constitute personal data if they are in the hands of an internet access provider (C-70/10). Whether this also applies to IP addresses stored by internet service providers has not been decided yet, but the question has been filed with the European Court of Justice (C-582/14) and a decision on the matter can be expected in the summer of 2016.

§ Profiling for automated individual decision-making purposes

The Regulation imposes specific requirements for automated individual decision making processes (Article 22). These apply, in particular, where decisions are based solely on automated processing, including so-called profiling. The term “profiling” has been defined broadly, such that it may cover selections made for dialogue marketing purposes (Article 4(4)). However, the Regulation only imposes specific requirements to automated individual decisions, if such decisions produce legal effects concerning the data subject or similarly significantly affect him or her.

Selections for dialogue marketing purposes are made in order to select addressees of persons who are potentially interested in advertised products and services. Such selections do not have any legal effect or significant adverse consequences for the data subjects. Therefore, Article 22 does not apply to dialogue marketing. The processing of personal data for selection purposes only needs to comply with the general legal requirements.

ALTERNATIVE 1: BALANCE OF INTERESTS

The Regulation allows the processing of personal data for the purposes of legitimate interests pursued by the advertiser "except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data" (Article 6(1)(f)). The reference to "processing" means, in particular, the collection, storage, use or disclosure by transmission of personal data (Article 4(2)). Thus, the legal basis applies to the processing of personal data for dialogue marketing purposes, including the collection and selection of as well as the actual contacting of the addressees.

The Regulation makes it clear that: "The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest" (Recital 47). This is in line with the current European Data Protection Directive. The Regulation also provides an unconditional right for data subjects to object to dialogue marketing. This will allow an addressee to ban advertisers from contacting him or her at any point in the future (see Section 2.2 of this Best Practice Guide).

In the national implementing laws of the European Data Protection Directive in the Member States, the balance-of-interests clause has sometimes been amended or replaced by more specific provisions relating to dialogue marketing. There is legitimate doubt as to whether such restrictive provisions are compliant with the European Data Protection Directive. The Court of Justice of the European Union has already declared invalid such a provision in the Spanish data protection law (C-468/10 and C-469/10) and another related case on a similar request is pending (C-582/14).

The Regulation's approach to the use of data for dialogue marketing purposes remains to be based on a balance-of-interests clause. However, the balance of interest approach does not apply where the data subject objects to the use of his or her data for dialogue marketing purposes (see Section 2.2 of this Best Practice Guide) or where special categories of data are processed. The Regulation clarifies that higher standards apply with regard to the processing of data relating to data subjects under the age of 16 years.

The data subject may have an overriding interest in the protection of his or her data where especially comprehensive or sensitive sets of data are transmitted. This type of scenario does not normally arise in dialogue marketing, since the selection criteria are aggregated prior to the transmission of the data. Furthermore, the assessment also needs to take into account whether the data are technically protected against special risks. Pseudonymisation is one way to protect data against such risks.

Any assessment of data protection measures by the advertiser should take into account whether a data subject can reasonably expect, at the time and in the context of the collection of the personal data, that processing for dialogue marketing purposes may take place (Recital 47). Where an advertiser has made commercial contact with the data subjects, it can be assumed that the data subject has a reasonable expectation that his or her data will be processed for such purposes. The general expectations of how the data will be used for dialogue marketing purposes usually exceed the actual use made of such data for dialogue marketing purposes. However, the advertiser should always provide specific data privacy information to the data subjects in this regard, so that they know exactly what to expect.

The balance-of-interests clause explicitly states that interests of third parties may be taken into consideration during the assessment process. This is important where the advertiser does not hold the data itself, such that other market participants or data service providers may refer to the advertiser's legitimate interest. This is especially important where data are disclosed to the advertiser.

In order to make it easier to contact addressees or to select data, any data retrieved from other market participants, publicly available sources or data service providers may be combined with existing data, so long as the interests of the data subject are sufficiently protected.

The processing of special categories of data (Article 9) or of data relating to criminal convictions and offences (Article 10) for dialogue marketing purposes is prohibited unless the data subject's consent has been obtained. Special categories of data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (Article 9(1)).

The provision on automated individual decisions (Article 22) does not prohibit the application of the balance-of-interests clause for dialogue marketing purposes. As noted above, the selection of data for dialogue marketing purposes, whether or not by means of profiling, does not produce legal effects concerning the addressee or similarly significantly affect him or her.

The balance-of-interests approach is used in order to weigh the legitimate interests of the data subject against those of the data processor or advertiser. The Regulation expressly respects the freedom to conduct business (Recital 4). However, the Regulation takes into

account various other fundamental values; for example, where dialogue marketing is undertaken for fundraising purposes, the public interest in such marketing will be relevant.

The following examples illustrate how interests may be balanced:

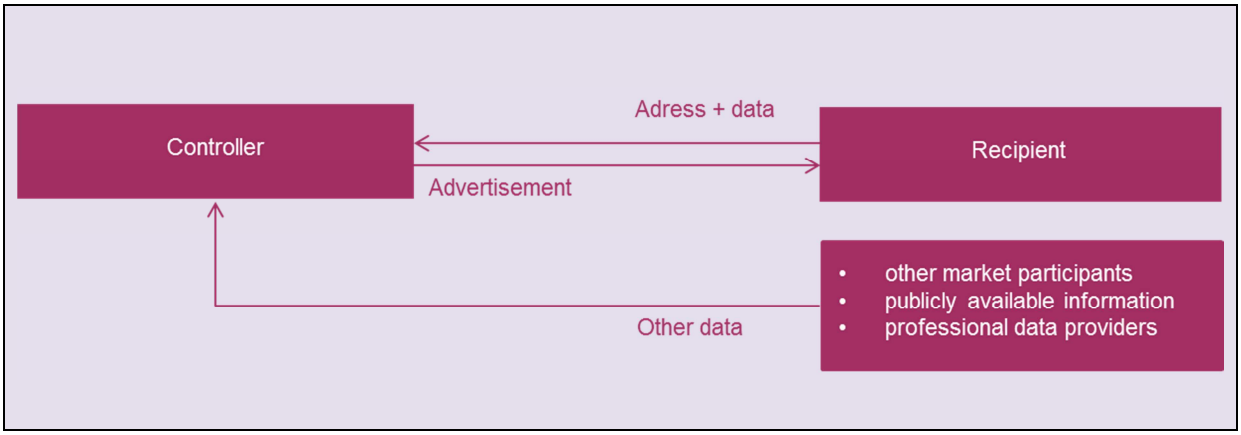
EXAMPLE 1: APPROACHING POTENTIAL AND EXISTING CUSTOMERS

Companies receive personal data from interested persons who directly contact the company or from persons already buying the company's products or services. The data sets contain information about the channels through which the person may be contacted and about the products and services in which the person has shown an interest. Other selection criteria, for example from other market participants, publicly available sources or data service providers, may be added to the data set.

A company has a weighted legitimate interest in processing personal data for dialogue marketing purposes in order to maintain its business relations with potential or existing customers.

In these scenarios, the data subject's interests usually do not merit special protection. The addressee has contacted the company. Thus, the receipt of advertising material can be reasonably expected as long as the data subject has not objected to the use of his or her data for such purposes. The use of selection criteria helps the advertiser to contact the data subject according to his or her specific interests.

Where data are disclosed for dialogue marketing purposes, one always needs to take into account that, so far, there has not been any commercial contact with the receiving advertiser when assessing the data subject's interests in protection. This is especially true for B2C contacts. Higher-ranking legitimate interests on the part of the consumer may, for example, be compensated through aggregation or pseudonymisation of selection criteria, so that the balance-of-interests clause can be used as a legal basis for data processing in those cases.

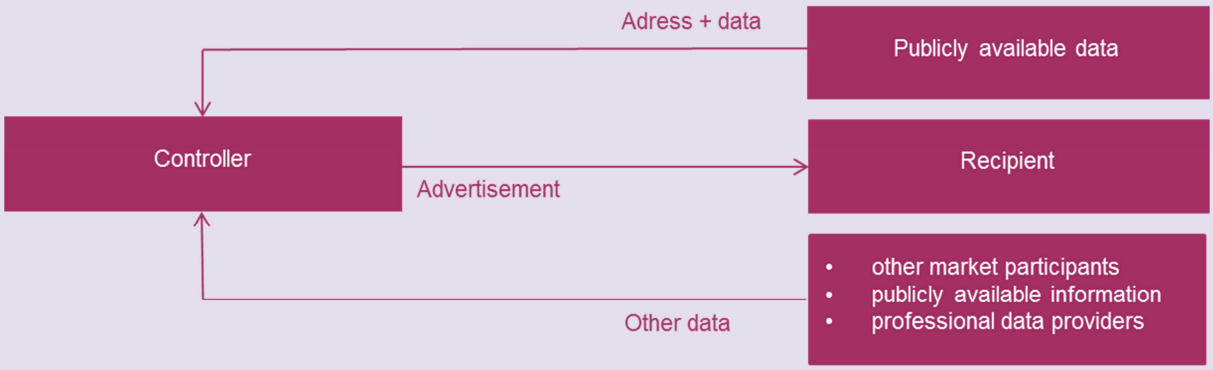


EXAMPLE 2: PUBLICLY AVAILABLE DATA

Advertisers and data service providers collect data from publicly available sources for dialogue marketing purposes. They have a legitimate interest in doing so. The data are either used to acquire new customers or to complement selection criteria. The data are either collected from publicly available sources by the advertiser itself or by data service providers.

The companies' interest in the acquisition of new customers is a weighted one, since a company cannot succeed in the long term if it caters only to its existing customers. The combined data are also important for the maintenance of existing customer relationships, because such data facilitates the creation of meaningful selection criteria.

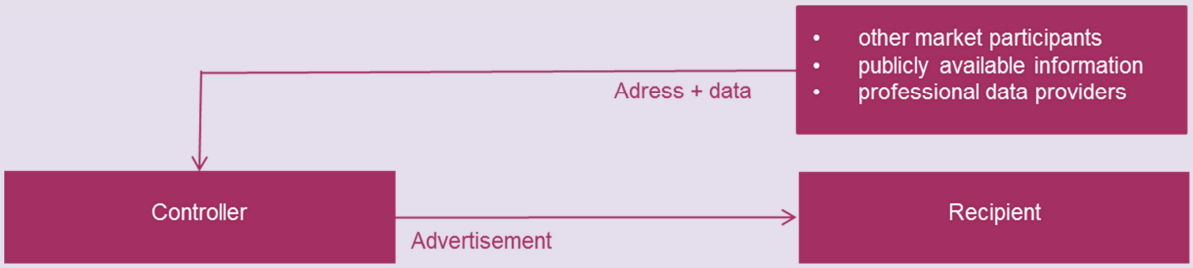
The data subject's interest in the protection of such data is normally rather low, since the data are already public and available to anyone world-wide. Where an objection to the use of such data has been published (such as in imprint data on the internet), such objection should be taken into account. Copyright restrictions may apply if the data are taken from legally protected sources.



EXAMPLE 3: B2B

The balance-of-interests clause does not explicitly differentiate between B2B- and B2C-customers. However, there is more flexibility regarding the processing of personal data for dialogue marketing purposes in the B2B-sector. Business addresses and the pertaining selection criteria can be collected directly from the addressee or they may be acquired from other market participants, from publicly available sources or from data services providers.

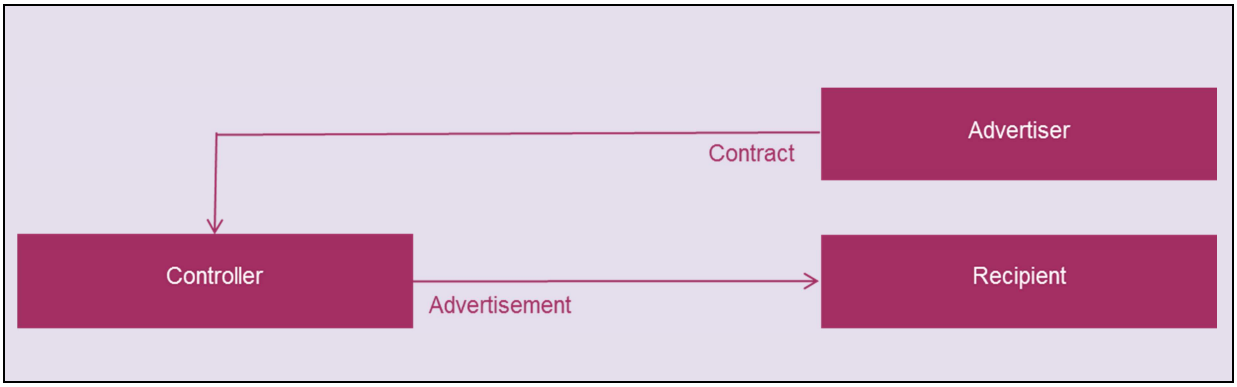
Where B2B-advertising is concerned, the selection criteria usually do not consist of personal data since the desired information concerns the company itself (such as information about the branch, business activities, turnover or requirements for subcontracted products). The protection afforded by the Regulation does not apply to the data of legal persons (Recital 14). However, advertisers should aim to exclude private data relating to the specific contact person.



EXAMPLE 4: RECOMMENDATIONS

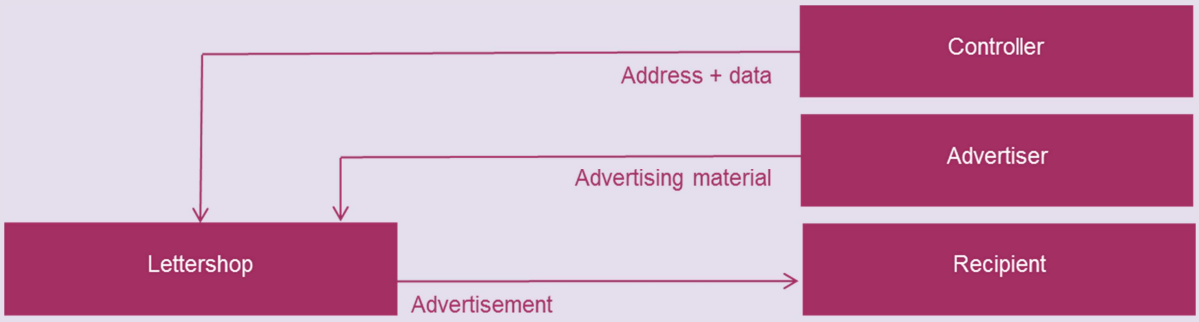
Companies support each other by recommending each other's products and services. In the context of balancing the interests of the parties, the interests of third parties (here, the recommended company) may be taken into consideration for the assessment.

Either the recommending company sends out the advertisements itself or it employs service providers as processors. It is not necessary to disclose the addressees' data to the recommended company.



EXAMPLE 5: LETTERSHOP

Dialogue marketing occasionally involves so-called Lettershop mailing. As in recommendation advertising, the processing of the customer data is either carried out by the advertiser itself (so-called list owner) or by a service provider (so-called Lettershop). However, unlike recommendation advertising, the address of the recommended company is shown as the sender address, but the recommending company is responsible for the selection and the contacting of addressees (although, as in recommendation advertising, the data of the addressees are not disclosed to the recommended company). The same criteria need to be considered in the balance of interests as in recommendation advertising.



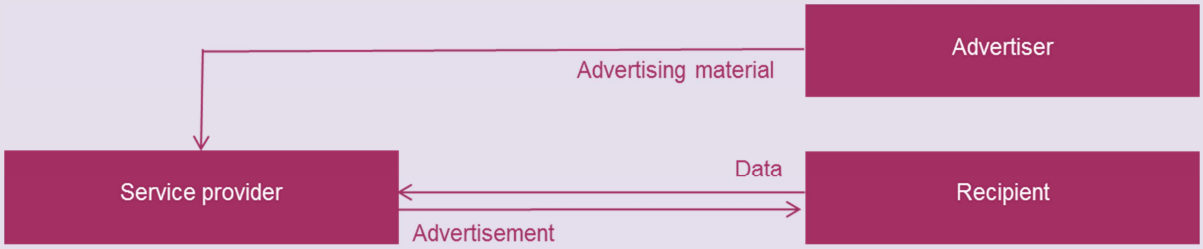
EXAMPLE 6: ONLINE BEHAVIOURAL ADVERTISING

The goal of Online Behavioural Advertising is to facilitate a tailored display of potentially interesting advertisements to users of online services. Particular categories of users are approached based on pseudonymized or anonymized selection criteria.

The providers of internet services as well as the advertiser have legitimate interests in displaying advertisements suitable to the needs and interests of their particular users. The revenue generated from this type of advertising is an important financial source for internet services. The advertiser

gains a valid communication channel to these users via online advertising. All of these factors can be taken into consideration in the balance-of-interests process.

Caution should be exercised where the data set is especially comprehensive or sensitive, in which case the legitimate interests of the user may outweigh those of the advertiser or internet service provider unless sufficient measures are in place to protect such data. Where service providers are used, it is important to ensure that the actual selection criteria are not directly disclosed to the advertiser. Pseudonymisation adds extra protection to personal data. Transparency and preference management increase the level of protection for the data subject's legitimate interests. In practice, where such methods are employed, the data subject will be sufficiently protected, such that the interests of the advertiser would normally outweigh those of the data subjects.



ALTERNATIVE 2: CONSENT

The processing of data for dialogue marketing purposes is also permitted under the Regulation if the data subject consents to it. However, the provisions on consent were negotiated specifically in light of the social media phenomena, which has led to a confusing and, in parts, inconsistent legal framework.

At first glance, the definition of the term "consent" does not appear to have changed fundamentally from the one in the European Data Protection Directive. However, the Regulation provides more detailed requirements for obtaining consent, some of which deviate from those enshrined in the national laws implementing the European Data Protection Directive. This creates a risk that existing declarations of consent might cease to be valid once the Regulation becomes applicable. Companies are advised to review and, where necessary, amend existing declarations as soon as possible to comply with the requirements of the Regulation.

REQUIREMENT	EXPLANATION	SOURCE
Freely given	Consent might be considered not freely given where: - performance of an agreement is conditional on a declaration of consent that is not necessary for the performance of that agreement; - there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority; - it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case.	**Article 4(11)** **Article 7(4)** **Recitals 42 and 43**
Specific	Consent should be valid for specific cases and should cover all processing activities carried out for the same purpose or for multiple purposes.	**Article 4(11)** **Recital 32**
Informed	The data subject should be aware at least of the identity of the controller and the purposes of the processing.	**Article 4(11)** **Recital 42**
Unambiguous	Consent must constitute an unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement,	**Article 4(11)** **Recital 32**

	by electronic means, or by an oral statement. Silence, pre-ticked boxes or inactivity cannot constitute consent.	
Demonstrable	The controller should be able to demonstrate that the data subject has given consent to the processing operation.	**Article 7(1)** **Recital 42**
No unfair terms	Reference to limitations regarding unfair terms in consumer contracts (including Directive 93/13/EEC).	**Recital 42**
Notice about the right to withdraw	Prior to giving consent, the data subject must be informed of his or her right to withdraw consent.	**Article 7(3)**
Clearly distinguishable and in an intelligible and easily available form, using clear and plain language	The data subject should be made aware of the fact that their consent is required, particularly in the context of a written declaration which concerns the processing of personal data in addition to other matters.	**Article 7(2)** **Recital 42**
Authorisation by the holder of parental responsibility of a child	Applies only where data subject is under the age of 16 years. Member States may provide by law for a lower age, as long as it is not below the age of 13 years.	**Article 8**
Explicit	Applies only to consent in the processing of special categories of personal data, automated decisions	**Article 9(2)(a)** **Article 22(2)(c)**

	and transfers to third countries.	**Article 49(1)(a)**
Clear, concise and not unnecessarily disruptive to the use of the service	Applies only to consent given following an electronic request to process data.	**Recital 32**

The diverse requirements of the Regulation for valid declarations of consent will, in practice, cause substantial legal uncertainty. Therefore, companies should as a first step determine whether consent is required. In many instances, it will be easier to work with another legal ground such as the balance-of-interests clause.

Certain of the Recitals illustrate the requirements for valid consent with practical examples. Recital 32 specifies that ticking a box when visiting an internet website constitutes valid consent, whereas silence or pre-ticked boxes does not.

§ Consent as an additional safeguard

Advertisers may want to obtain the consent of data subjects as an additional legal safeguard. Should consent be withdrawn, invalidated or insufficiently verifiable, the company may still be able to rely on a different legal basis for the processing of personal data. The concept of recourse to other legal grounds is expressly mentioned in respect of the so-called “right to erasure (‘right to be forgotten’)” (Article 17(1)(b)). Therefore, one can argue that if an existing declaration of consent fails to meet the requirements of the Regulation, recourse to other legal grounds is admissible.

§ Consent to communicate via electronic means

Where electronic means are used to contact a data subject, the ePrivacy Directive requires the consent of the data subject in certain circumstances. The Regulation makes it clear that it does not intend to impose additional obligations in relation to matters – where communication services are already subject to specific obligations with the same objective set out in the ePrivacy Directive (Article 95). This will apply at least until the ePrivacy Directive is reformed. Therefore, the national implementation laws remain in place for the time being. However, they only remain valid to the extent that they do not exceed the restricted scope of application of the ePrivacy Directive to electronic communications services in public

communication networks in the European Union.

The processing of personal data necessary for the preparation of advertising by email can usually be justified under the balance-of-interests clause. Pursuant to the ePrivacy Directive, it is sufficient if the consent to electronic advertising refers only to the possibility to communicate with the individual by email. Data subjects should be informed whether the advertisement relates only to products or services offered by the advertiser itself, or also to those of third party companies. If consent for third party emails is being sought from the data subject, this should be expressly stated.

§ Unambiguous or explicit consent

The Regulation distinguishes between unambiguous and explicit declarations of consent. The data subject must give explicit consent to the processing of special categories of personal data (Article 9), to automated decisions (Article 22(2)(c)) and to the transfer of such data to third countries (Article 49(1)(a)). Therefore, for dialogue marketing purposes, explicit consent will only be required in exceptional cases. However, as stated above, silence, pre-ticked boxes or inactivity do not constitute “unambiguous” consent. Depositing a business card at a trade fair, for example, should constitute valid consent for communicating with the individual under the Regulation.

§ Limited prohibition on coupling

The Regulation requires that: “When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, […], is conditional on consent […]” (Article 7(4)). Consent shall only be presumed to have been given freely if there is a genuine or free choice. It must be possible for the data subject to refuse or withdraw his or her consent without detriment (Recital 42). For different personal data processing operations, separate declarations of consent should be collected (Recital 43).

These requirements, taken together, appear to impose limitations on coupling of contracts with consent. However, the provision states that it shall not apply where the consent is necessary for the performance of a contract. The exemption does not refer to constellations in which the processing of data is necessary for the performance of a contract, because in such instances, no consent is required, in any case (Article 6 (1) (b)). The provision refers to constellations in which consent is necessary for the performance of a contract. Examples are lotteries, coupons or other special benefits which are granted in exchange for a declaration of consent. It also applies if a service is financed by data processing based on consent.

§ Consent by a child

Where a child is below the age of 16 years, consent to data processing in connection with an information society service shall be lawful only if and to the extent the consent is given or authorised by the holder of parental responsibility over the child (Article 8). Member States may lower the age level, provided that it is not below the age of 13 years. As a result, this provision is likely to create inconsistencies in the approach of different Member States within the European Union. Further, providers offering services to children below the age of 16 years will hardly be able to determine whether or not consent has been given or authorised by the child's legal guardian.

As a first step, advertisers should determine whether consent is required. The legitimate interests of children receive high priority in any balance of interests, as is expressly stated in Article 6(1)(f). However, the balance of interests may be considered as an alternative to obtaining consent, provided that the legitimate interests of the data subject are carefully assessed.

ALTERNATIVE 3: COMPATIBLE PURPOSES

A further legal ground for the processing of data exists where data initially were not collected for dialogue marketing purposes, but the processing for dialogue marketing purposes is not incompatible with the initial purpose (Article 5(1)(b) and 6(4)). In such a case, no legal ground separate from that which allowed the collection of the personal data is required for the further processing (Recital 50).

In dialogue marketing, the clause regarding compatible purposes is of limited implications, since, in a commercial context, data are collected for dialogue marketing purposes as well. Thus, the purpose does not need to be amended at a later stage. To the extent to which data are used for statistical purposes (such as for Big Data applications) but has not been collected for such purpose, the change of purpose is considered to be compatible with the initial purposes (Article 5(1)(b)).

In the rare case in which the use of data for dialogue marketing requires a change of purpose, any new purpose must be matched against the initial purpose of the processing. The Regulation lists five criteria which constitute in essence a specific kind of balance of interests and which should, in most circumstances, justify the processing of data for dialogue marketing purposes (Article 6(4)).

§ Can a change of purpose be justified on the basis of the balance-of-interests clause?

In the initial draft of the Regulation, the European Commission suggested inserting a provision that would have prohibited the use of the balance-of-interests clause to justify a change of purpose where the new purpose was "incompatible" with the initial purpose. However, the suggested provision was deleted in the course of negotiations, with the result that the Regulation preserves the status quo established by the European Data Protection Directive on this issue.

The legal concept of change of purpose operates as follows: If the change of purpose for the processing is compatible with the initial purpose for the processing, there is no need to establish an additional legal basis for the further processing. However, if the further processing is incompatible with the initial processing, then the further processing is not admissible unless it can be justified on an alternative ground. Therefore, even if the initial purpose for a processing was not dialogue marketing, the processing may be justified via the balance-of-interests clause.

In light of the contentious negotiations regarding purpose limitation in the draft Regulation, it is expected that this issue will give rise to diverging opinions. The advocates of a strict purpose limitation will be likely to oppose any interpretation allowing recourse to the balance-of-interests clause to justify a change of purpose. However, Recital 50 states that a change of purpose that is compatible with the initial purpose for processing does not require any additional legal ground. This creates a two-tier model (a 1st tier without specific legal basis and a 2nd tier with specific legal basis), which suggests the possibility to take recourse on other legal grounds.

Given that an "incompatible" change of purpose will only exist in rare cases, the potential controversy on this issue is not a crucial factor in practice for dialogue marketing.

2.2 RESPECTING THE OBJECTION OF AN ADDRESSEE

Since the Regulation, in principle, retains the Opt-out Principle for the processing of data for dialogue marketing purposes, the provision on the right to object is of major importance (Article 21 and Recital 57). If the data subject objects to the processing for dialogue marketing purposes, the controller shall no longer process his or her personal data for such purpose. The right to object shall be brought to the attention of the data subject no later than the time

of the first communication with the data subject (Article 21(4)). The information must be presented clearly and separately from any other information (see Section 3 of this Best Practice Guide for detailed examples of such notifications).

If an addressee objects to the use of his or her data for marketing purposes, such objection needs to be strictly respected. Advertising material must not be sent to anyone against their will. The data subject's right to self-determination overrides any potential interests of the advertiser or a third party. To the extent that general *ad denier* lists are compiled, such as for the so-called Robinson list of the DDV, any person filing an objection with a company should be informed of the existence of such a list.

If an advertiser receives an objection from a data subject, it is important to determine the exact intention of the data subject in order to respond appropriately. In practice, the types of objections filed by data subjects are of unlimited variety and a good deal of interpretation is required to determine a data subject's intention with any certainty.

Example 1: "I do not wish to receive marketing material from you."

This objection is directed at the advertiser. One option for complying with such an objection is to include the address of the objecting data subject into an internal *ad denier* list. The data in the list are maintained in the data subject's interest. The data subject should be informed about being included on the list. New mailings should always be checked against the *ad denier* list. There is no guarantee that, due to typical matching errors that can occur in connection with such lists, objecting data subjects will not accidentally receive mailings on occasion. However, the advertiser cannot be expected to apply more than reasonable diligence.

Example 2: "I do not wish to receive marketing material from firms with which I have no dealings."

Upon receipt of an objection, the advertiser should include the objecting data subject on an internal *ad denier* list and, in addition, ensure that the data subject's address data are no longer made available to third parties. The data subject should be notified regarding his or her inclusion on such list.

Example 3: "Please delete my data."

Data subjects often demand the deletion of their data in order to avoid receiving further marketing materials. In this case, the advertiser should include him or her on the *ad denier* list. Subsequently, the advertiser should inform the data subject that a permanent cessation of mailings cannot be achieved by deletion, but by blocking of data, since deletion of his or her

personal data would lead to a removal from the *ad denier* list and consequently not achieve the data subject's initial goal. The advertiser should then request that the data subject contacts the company once more to confirm whether he or she wishes for all of his or her personal data to be deleted, including personal data in the company's *ad denier* list.

2.3 GENERAL PROCESSING PRINCIPLES

The Regulation contains a number of principles relating to processing of personal data (Article 5). These are specified through the detailed provisions of the Regulation. Therefore, they do not have much weight on their own. However, one must be able to demonstrate compliance with such principles (Article 5(2)). Companies in the dialogue marketing sphere should especially note the following:

Lawfulness, fair processing, and transparency

Personal data may only be processed lawfully, fairly and in a transparent manner in relation to the data subject. Companies must observe the specific requirements for lawfulness and transparency in order to comply with this principle (see Section 2.3 and 3 of this Best Practice Guide).

Purpose limitation

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Since, in a commercial context, data are collected for dialogue marketing purposes, there is usually no later change of purpose (see Section 2.1 Alternative 3 of this Best Practice Guide). Therefore, this principle is of minor importance in the context of dialogue marketing. However, companies should ensure that data subjects are informed that the initial purposes for collecting their personal data include the processing of such data for marketing purposes.

Data minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Where personal data are processed for dialogue marketing purposes, it is important to check that the processed data are adequate and relevant for mailing and selection.

Accuracy

Personal data shall be accurate and, where necessary, brought up to date. Every reasonable step must be taken to ensure that personal data are accurate. With regard to dialogue marketing, the measures for erasing, rectifying and updating the addresses of data subjects are particularly important. These measures must be individually assessed to determine their adequacy, which may depend in part on external factors such as the availability of data validation and correction services by external service providers under adequate terms.

Duration of storage

The identification of data subjects shall be permitted for no longer than is necessary for the purposes for which the personal data are processed. Dialogue marketing necessarily requires the contacting of addressees, and consequently the identification of particular data subjects. For selection purposes, pseudonymised sets of data can be used. However, selection will usually also require the identification of data subjects. Data storage is no longer necessary when the data no longer has advertising potential. It is almost impossible to set standardised time limits. However, when an addressee has not reacted to any mailings for a consistent period of time, his or her data should no longer be used for dialogue marketing purposes. The advertiser has various obligations to inform data subjects regarding the duration for which their data are stored (see Section 3.1 of this Best Practice Guide), including specific obligations concerning the deletion of such data (though there are no specific provisions regarding time limits for the storage of personal data). However, the limitations can be expressed in general terms and do not need to set a fixed time frame.

Integrity and confidentiality

Personal data shall be processed in a manner that ensures appropriate security of the personal data. The Regulation imposes specific data security measures (Article 32) requiring that companies implement appropriate technical and organisational measures. In doing so, the state of the art and the costs for the implementation along with the kind, scope, circumstances, as well as the purpose of and the risk involved with the processing need to be taken into account. Where data subjects' addresses alone are being processed, the requirements are lower than where such addresses are processed with comprehensive and sensitive selection criteria.

2.4 DATA PROCESSING WITHIN A GROUP OF COMPANIES

The Regulation does not treat transfers of data between group companies in the same way as transfers within a single entity. From a data privacy perspective, each company in a group of companies is treated as a separate entity. The operation of intra-group Customer Relationship Management systems (CRM systems) and the use of the generated data for dialogue marketing purposes can be based on the balance-of-interests clause or on group-level consent. The Regulation concedes that group companies have a legitimate interest in transferring personal data within the group (Recital 48).

Where interests are balanced against each other in an intra-group context, the legitimate interests of the company usually outweigh those of the data subject. This is to be contrasted with a scenario in which personal data are transmitted to external entities. In this case, the legitimate interests of the data subject generally have more weight.

The Regulation also provides for a scenario in which two or more companies jointly determine the purposes and means of processing as joint controllers (Article 26). In such a scenario, the participating companies should formalise their respective obligations under this Regulation by means of an agreement. This can be an appropriate solution in the case of an intra-group CRM system. As an alternative, the CRM system may also be managed by a contracted service provider (see Section 4 of this Best Practice Guide). Alternatively, companies may find that some combination of the solutions stated above is but suitable for them.

3. PROVIDING COMPREHENSIVE TRANSPARENCY

3.1 GENERAL OBLIGATIONS TO INFORM

The Regulation imposes different obligations where data are collected directly from the data subject (Article 13) as opposed to being collected from other sources (Article 14). Considering it is easier to inform the data subject of the processing if the data are collected directly from the data subject, the obligation to inform is stricter than in a situation where the data are collected from other sources.

The Regulation also differentiates between a minimum level of information, which must always be provided to the data subject, and additional information which needs only to be provided to the data subject if it is necessary or required for a fair and transparent processing of the data. The trigger for the provision of additional information is rather unclear and, as a

result, does not promise legal certainty. Therefore, companies are advised to provide comprehensive information wherever this does not pose any technical or other problems (for example, by including data privacy information on a website).

Recital 58 expressly states that the information can also be provided to the data subject in electronic form, for example, through a publicly available website. Hence, information can be provided in a layered approach. For example, the minimum level of information can be provided in a mailing, and for all additional information, including information which changes frequently (such as the contact details of the data privacy officer, the list of data receiving group companies or the categories of other potential data recipients) can be provided through a website.

It is recommended that the data subject is notified regarding the right to object to the use of his or her personal data for marketing purposes at the earliest stage possible, even in cases where it would also be sufficient to do so at the time of the first communication (Article 21(4)). Where the consent of the data subject has been obtained, the mandatory minimum information must be provided at the time consent is obtained (see Section 2.1 of this Best Practice Guide).

The extent to which the data subject is already aware of the mandatory minimum information, there is no need to provide such information again (Articles 13(4) and 14(5)(a)). However, while it may be considered common knowledge that, in a commercial context, the purposes of collection of personal data include dialogue marketing, companies are advised to always provide the mandatory minimum information at the point of first contact with the data subject. Where possible, the right to object should also be expressly stated in each mailing, and presented clearly and separately from any other information (Article 21(4)).

EXAMPLE 1: An advertiser uses the addresses of its own customers and of interested persons in order to advertise its own products and services. Furthermore, the advertiser intends to make such data available via a Lettershop for third parties' mailings. The company should inform the data subjects of this purpose and their right to object to it at the point that their data are initially collected.

SUGGESTED WORDING:

"Privacy Notice: We wish to maintain our relationship with you as a customer and to provide you with information and offers regarding products and services. Under Article 6(1)(f) of the General European Data Protection Regulation, we will process your personal data (in some cases, with the help of service providers) in order to send information and offers from

us and from other companies to you. If you do not wish to receive such information or offers, you may object to the use of your data for marketing purposes at any time. Please feel free to contact us at our address. [OPTIONAL: You may also send your objection via e-mail to: E-MAIL ADDRESS.] For further information regarding data protection, please see [INTERNET LINK LEADING TO COMPREHENSIVE DATA PRIVACY INFORMATION]. You can reach our Data Protection Officer at our address."

3.2 INFORMATION TO BE PROVIDED IN A MAILING

At the time of the first communication to the data subject, such data subject has usually already been notified with some or all of the mandatory minimum information. Such parts may be omitted from the information provided with the first communication. However, since the right to object constitutes the central legal justification for mailings sent out without consent, the information concerning such right should be provided with each and every mailing.

Where a company (i.e. list owner) sends out mailings on behalf of a third party via a Lettershop, the information of the advertiser should always be included (see Example 1). Thereby, the addressees will be sufficiently informed of the purpose for the data collection and their right to object before they contact the advertiser regarding the mailing.

If an addressee objects to the processing of his or her personal data as a result of a mailing sent out via a Lettershop, the advertiser must respect such objection. Furthermore, the advertiser should inform the company who sends out the mailing of the objection to ensure that the particular data subject's address is not used in any future Lettershop mailing.

Where data are not collected directly from the data subject (but, for example, from publicly available sources, other market participants or data service providers), the initial communication will usually provide the first opportunity of informing the data subject without disproportionate effort (Article 14). The information provided must be comprehensive and must also contain information on the right to object.

EXAMPLE 2: An advertiser collects data from a publicly available source and uses it for advertising campaigns.

SUGGESTED WORDING:

"**Privacy Notice:** We would like to win you as a customer, to maintain our relationship with you as a customer and to provide you with information and offers regarding products and services. Under Article 6(1)(f) of the General European Data Protection Regulation, we will process your address data and criteria for tailored advertising (in some cases, with the help

of service providers), in order to send information and offers from us and other companies to you. If you do not wish to receive such information or offers, you may object to the use of your data for marketing purposes at any time. It will help us to process your objection more quickly if you enclose the advertising material you received. Please feel free to contact us at our address. [OPTIONAL: You may also send your objection via e-mail to: E-MAIL ADDRESS.] For further information regarding data protection, please see [INTERNET LINK LEADING TO COMPREHENSIVE DATA PRIVACY INFORMATION]. You can reach our Data Protection Officer at our address."

3.3 DATA BREACH NOTICE

The Regulation sets out the circumstances in which a data controller has an obligation to notify regulatory authorities and the relevant data subject if a breach of personal data occurs (Articles 33 and 34). The data controller shall without undue delay and, where feasible, not later than 72 hours after having become aware, notify the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons (Article 33(1)). When the personal data breach is likely to result in a "high" risk to the rights and freedoms of natural persons, the controller shall also communicate the personal data breach to the data subject without undue delay (Article 34(1)).

An advertiser will need to implement internal organisational measures in order to sufficiently comply with such obligations. Each employee within the company should know that he or she must report any data breaches, and to whom he or she must report any such breaches. Service providers shall be obliged to report any breaches coming to their knowledge to ensure that the company is able to report to the relevant party in time.

4. CONTRACTING SERVICE PROVIDERS SECURELY

4.1 COMMISSIONED DATA PROCESSOR

The Regulation allows companies to use Lettershops and other service providers as so-called processors acting under the authority of the controller (Article 28). The disclosure of data to such processors does not count as a disclosure to third parties (Article 4(10)). The relationship between controller and processor is applied as if the processor were part of the controller. The same is true for the sub-contractors of each service provider. In this way, the

Regulation tries to ensure that the data privacy regime does not unnecessarily hinder the division of labour between advertisers and service providers.

The concept protects the data subject and facilitates the legal use of service providers. If, for example, a mailing is sent out via a Lettershop, the data subjects' addresses are not disclosed to the advertiser. Instead, the list owner contracts with the service provider (Lettershop or another service provider) as processor. In this way, the list owner remains the controller with respect to the processing of the data.

However, where independent responsibilities for determining the purposes and means of the data processing are transferred, the processing can no longer be defined as a sub-contracted processing. The distinction between dependent and independent provision of services is rather vague. Lettershops and other service providers are seen as processors, if the controller alone decides on the purposes and means of the data processing. Therefore, it is important to underline that list owners decide on the use of their data on their own.

4.2 MINIMUM CONTRACTUAL REQUIREMENTS

The contract with the processor shall set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller (Article 28(3)). In addition, provision must be made for at least the following issues:

- Documented instructions from the controller

- Confidentiality obligations of the persons authorized to process the personal data

- Security measures to be taken

- Further subcontracting of processors

- Rights of the data subjects

- Processor's assistance in complying with controller's obligations

- Deletion or return of the data following termination or expiry of the sub-contract

The DDV has incorporated the special requirements for contracted data processing into its quality and performance standards (*Qualitäts- und Leistungsstandards - QuLS*). In addition, the DDV makes its Declaration of Commitment (*Verpflichtungserklärung*) available as a model text to members and non-members alike. The quality and performance standards as

well as the DDV Declaration of Commitment will be revised to comply with the provisions of the Regulation.

Until 25 May 2018, when the Regulation becomes applicable, companies are advised to agree terms with contractors to apply through 24 May 2018 and to replace the old provisions as of 25 May 2018. This will significantly reduce the volume of transition work in the lead-up to 25 May 2018.

DDV members who have committed themselves to the above DDV Declaration of Commitment are listed on the DDV website (www.ddv.de). They are regularly audited by the DDV in the course of controlling compliance with its quality and performance standards.

4.3 RESPONSIBILITIES OF THE SERVICE PROVIDER

The Regulation expands the service providers' responsibilities. For example, service providers shall maintain a record of all categories of processing activities carried out on behalf of a controller (Article 30(2)) and co-operate, on request, with the supervisory authority in the performance of their tasks (Article 31). In addition, the data subjects may make direct liability claims against the processor. The supervisory authorities may impose sanctions. The contractual relationship between principal and the services provider needs to take these changes of responsibilities into account.

5. IMPLEMENTING DATA PROTECTION EFFECTIVELY

5.1 KEEPING A RECORD OF PROCESSING ACTIVITIES

Companies and their service providers must retain control over their data processing activities. To this end, the Regulation requires companies and service providers to keep a record of their processing activities. Companies with less than 250 employees are exempt from this rule, unless the processing that is likely to result in a risk to the rights and freedoms of data subjects, is not occasional, or includes special categories of data (Article 30(5)). In the area of dialogue marketing, most of the companies and service providers employ less than 250 employees. The processing, however, is usually "not occasional". Therefore, the obligation to keep a record of processing activities will often apply.

The requisite record may be kept in electronic form (Article 30(3)). It must be made available to the supervisory authority upon request. The Regulation does not require registration of

data processing with, or notification of data processing to the responsible supervisory authorities. There is no general public right of access to the record of data processing.

5.2 DATA PROTECTION OFFICER

The Regulation requires the designation of a data protection officer in certain cases (Article 37). The obligation is triggered by the core activities of the company, rather than the number of its employees. A data protection officer must be designated if the core activities of the company require regular and systematic monitoring of data subjects on a large scale or consist of processing on a large scale of special categories of data. This is usually not applicable in the context of dialogue marketing. However, it may be advisable to designate a data protection officer or at least to appoint a person in charge of data protection, in order to assign the tasks related to data protection issues internally.

The Regulation gives Member States the choice to extend the obligation to designate a data protection officer. It remains to be seen whether, and to what extent, the Member States will make use of this option.

5.3 TECHNICAL AND ORGANISATIONAL MEASURES

Although many companies implement general technical and organisational measures to protect their data in the ordinary course, the Regulation obliges them to do so with regard to the processing of personal data (Article 32). Whether such measures are appropriate to ensure a level of security appropriate to the risk will depend on the state of the art, the costs for the implementation and the related risks. These measures are regularly audited by the DDV in the course of monitoring compliance with its quality and performance standards.

5.4 DATA PROTECTION IMPACT ASSESSMENT

The Regulation obliges companies to carry out a data protection impact assessment prior to introducing a new type of data processing, and to document such assessment in certain cases (Article 35). This applies to types of processing that are likely to result in a high risk to the rights and freedoms of natural persons. Normally, this will not apply to dialogue marketing activities.

5.5 ROLE OF THE SUPERVISORY AUTHORITIES AND THE EUROPEAN DATA PROTECTION BOARD

The Regulation assigns far-reaching tasks (Article 57) and powers (Article 58) to supervisory authorities. Among other things, the authorities shall cooperate on a European level and

coordinate their positions through a newly established body, called the European Data Protection Board (Article 68), which will replace the Article 29 Working Group.

The Regulation sets out a comprehensive regime of fines for possible data breaches (Article 83). For example, administrative fines of up to EUR 20 million, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year. Whichever is higher, can be imposed for breaches of the Regulation.

5.6 CONSUMER PROTECTION

Data subjects shall have the right to mandate organisations, in particular, consumer protection organisations, to exercise rights under the Regulation on behalf of the data subject (Article 80(1)). The Regulation also gives Member States the option to grant to such organisations the power to bring a formal action if it considers that the rights of data subjects have been infringed as a result of processing, even if such organisation has not been mandated to do so by a data subject (Article 80(2)). The provisions of the Regulation are without prejudice to further rights of organizations specified under other provisions (for example, with respect to general terms and conditions). Consumer protection organisations are not bound by decisions of the European Data Protection Board or national supervisory authorities.

5.7 CODES OF CONDUCT AND CERTIFICATIONS

Under the Regulation, national and European regulatory authorities shall encourage the preparation of codes of conduct and the establishment of certification mechanisms (Articles 40 to 43). However, these mechanisms are subject to detailed formal and procedural requirements. It remains to be seen whether codes of conducts and certifications will provide solutions in practice.

The DDV has enforced a strict regime of quality and performance standards for address service providers since 1992, and has continued to further develop it on an ongoing basis. In addition to meeting these quality and performance standards and conducting regular and independent controls, DDV members are also asked to carry out voluntary data privacy audits with strict audit criteria. Only companies that meet the DDV's standards are entitled to carry a quality seal certifying that the above audit has taken place.

6. ADEQUATE PROTECTION FOR CROSS-BORDER PROCESSING

6.1 UNIVERSAL PROTECTION

The territorial application of the Regulation is broad (Article 3(1)). Where the processing is carried out in the context of an establishment of a controller or processor in the European Union, the Regulation applies. However, the Regulation will also apply where a company without an establishment in the European Union offers products or services (even if they are free of charge) to, or monitors the behaviour of data subjects located within the European Union (Article 3(2)).

The Regulation protects personal data independent of the data subject's nationality or his or her place of residence. If, for example, the data of an American citizen are collected, processed or used in Germany (i.e., his or her American address is bought by a German company and the company then sends a catalogue to him or her from Germany), the Regulation applies, even if such person has never set foot into Germany or the European Union.

6.2 FREEDOMS WITHIN THE EUROPEAN UNION

The Regulation prohibits data privacy-related restrictions to the free flow of personal data between Member States. This applies to the whole of the European Union and will most probably also be adopted by the remaining countries within the European Economic Area (i.e. Norway, Iceland and Liechtenstein, but not Switzerland).

However, the free flow of personal data is subject to the general data processing requirements of the Regulation. The free flow of data only means that the restrictions imposed by the Regulation apply equally to data that is transferred from Munich to Hamburg as to data transferred from Munich to Paris – in both cases, the relevant parties must determine whether the transfer is permitted under the Regulation.

The provisions of the Regulation are complemented by the national rules implementing the ePrivacy Directive. As noted above, these rules continue to apply pending the expected reform to the ePrivacy Directive. This is particularly relevant in the context of electronic advertising, since such advertising is in most cases only admissible under the ePrivacy Directive with the consent of the addressee.

6.3 BORDERS OF THE EUROPEAN UNION

The freedom to transfer personal data within the European Economic Area is justified by the fact that for all Member States the same level of data protection is applicable under the Reg-

ulation. Only a small number of countries outside of the European Union have comparably strict data privacy laws. In light of the varying levels of protection granted in countries outside the European Union, the Regulation requires special measures for the transfer of data to so-called third countries. These special measures apply as long as the level of data protection in the third country is not approved as adequate in a decision by the European Commission. Where the Commission decides that the level of data protection is adequate, the same requirements for transfers of data transmission apply as for countries within the European Union.

If the level of protection provided in a third country has not been approved as adequate, the special restrictions for third country transfers need to be complied with. This also applies to the transfer of data to service providers in third countries.

It is important to note that the special requirements for third-country transfers apply in addition to the general requirements under the Regulation. If, for example, address data are to be transferred with selection criteria, as a first step, the company needs to determine whether or not such transfer would be admissible within the European Union. As a second step, the company will need to determine whether any special restrictions apply to the transfer of data to countries outside the European Union.

The European Commission has evaluated the level of data protection in a number of countries and found that Andorra, Argentina, Canada, Israel, New Zealand, the Eastern Republic of Uruguay and Switzerland, as well as the British Channel Islands of Guernsey and Jersey, the Isle of Man and the Danish Faroe Island grant an adequate level of protection (although certain of these jurisdictions are subject to additional restrictions). Previously, the United States of America was also deemed to provide an adequate level of data protection to the extent that the receiving American company had committed itself to the Safe Harbor Privacy Principles. However, in 2015 the European Court of Justice declared the “Safe Harbor” decision of the European Commission to be invalid (C-362/14). A replacement regulation, the EU-US Privacy Shield, has been available since 1 August 2016.

The existing adequacy decisions of the European Commission remain valid under the Regulation. Furthermore, there may exist an adequate level of protection in countries which have not been evaluated by the European Commission as yet. However, under the Regulation, one can only rely on an official adequacy decision by the European Commission.

6.3.1 Binding corporate rules

One tool to guarantee an adequate level of data protection is the introduction of binding corporate rules. Such rules are required to be approved by the responsible supervisory authorities. Since the approval procedure tends to be a lengthy process, the rules of only a small number of companies have been approved to date. Therefore, binding corporate rules have played a minor role in practice. However, it appears that this model is gaining ground as an increasing number of companies have commenced the introduction of binding corporate rules.

6.3.2 Standard contractual clauses

If a finding concerning the adequacy of protection available in a third country has not been issued by the Commission, , the company disclosing the data may agree the so-called standard contractual clauses with the company receiving the data. The European Commission has approved some model contracts to this end, which are published at the following URL: <http://ec.europa.eu/justice/data-protection/index_de.htm>.

There are two types of standard contractual clauses. The first type is designed for the transfer of data from a controller to another company who will also function as a data controller (2001/497/EC or alternatively C(2004)5271). The second type is designed for the transfer of data from a controller to a processors (new version C(2010) 593). In practice, the standard contractual clauses are the most common method of making compliant transfers of data transmissions to third countries. They are particularly useful for the contracting of processors in third countries.

The contents of the standard contractual clauses can only be revised with approval from the responsible supervisory authority. Therefore, in practice, these clauses cannot be revised by companies and must be filled in like forms. The standard contractual clauses are intended to complement the commercial contractual provisions which are agreed in the context of the transfer of data.

6.3.3 Valid consent to the disclosure of data

The transfer of data to third countries may also be allowed if the affected data subject explicitly consents to the transfer. However, in practice there often is no realistic possibility of obtaining such consent. It requires that the text used to obtain consent from the data subject clearly states that the data subject’s personal data may be transferred to third countries. Furthermore, the text must include a warning regarding the possibility of an inadequate level of

data protection granted in the recipient country. The general challenges of obtaining consent also apply here (see Section 2.1, Ground 2 of this Best Practice Guide).

6.4 SPECIAL STATUS OF SERVICE PROVIDERS

The Regulation contains special provisions for service providers acting under the authority of a controller. Under certain circumstances, such service providers are to be treated as processors (see Section 4 of this Best Practice Guide).

The advantage of subcontracted processing lies in the fact that the controller is treated as the principal actor, and the processor is not treated as a “third party”.

Processing is frequently contracted to so-called Lettershops in order to prevent disclosure of data by the list owner to the advertiser. The Lettershop acts as processor on behalf of the list owner and the list owner continues to be the controller of the data under the Regulation.

The advantages of sub-contracted processing apply regardless of where the processor is located, whether in Germany or within another country of the European Union. For example, the Regulation will apply equally to a contract between a company in Germany and a Lettershop in Frankfurt or in Warsaw.

7. UNDERSTANDING TERMINOLOGY CORRECTLY

Address data
Data about how a person can be reached by postal mail, electronic mail or telephone.

Processor
A service provider processing personal data under the authority of the controller. The purposes and means of the processing are determined by the controller.

Data subject
The natural person whose personal data are processed.

Recommendation advertising
Advertisements for the products of a third party which a controller sends out or arranges to be sent out.

Lettershop
A service provider carrying out services such as production, packaging or mailing of advertising materials or other correspondence to a group of recipients under the authority of a controller.

List owner
A company that owns address data as controller and which makes such address data available to third parties for marketing purposes.

Publicly available sources
Sources which are available to the general public, such as publicly available internet sites or address, telephone, branch and similar directories.

Personal data
Any information relating to an identified or identifiable natural person (including identifiable pseudonymized data). However, this does not include data relating to a legal person.

Selection criteria
Certain data which companies use to select specific addressees from a comprehensive list of persons for marketing purposes.

Controller
Any natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data, such as for example, list owners, but not processors.

8. EXCERPTS FROM THE GENERAL DATA PROTECTION REGULATION

RECITAL 4

The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.

RECITAL 14

The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

RECITAL 26

The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

RECITAL 30

Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

RECITAL 32

Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

RECITAL 42

Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC (10) a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

RECITAL 43

In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject

and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

RECITAL 47

The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

RECITAL 50

The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing

should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

RECITAL 57

If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authen-

tication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.

RECITAL 58

The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

ARTICLE 4 Definitions

For the purposes of this Regulation:

(1) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

[…]

4. ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

5. ‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

[…]

10. ‘third party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data

11. ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

[…]

ARTICLE 5 Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

ARTICLE 6 Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objec-

tives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

ARTICLE 7 Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

ARTICLE 8 Conditions applicable to child's consent in relation to information society services

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the

age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

ARTICLE 9 Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

ARTICLE 10 Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

ARTICLE 13 Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22 (1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

ARTICLE 14 Information to be provided where personal data have not been obtained from the data subject

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide

the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(e) the right to lodge a complaint with a supervisory authority;

(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

(g) the existence of automated decision-making, including profiling, referred to in Article 22 (1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

ARTICLE 17 Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers

which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

ARTICLE 21 Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

ARTICLE 22 Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

ARTICLE 26 Joint controllers

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are

determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

ARTICLE 28 Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 32;

(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part,

on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred

to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

ARTICLE 30 Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of pro-

cessing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

ARTICLE 32 Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

ARTICLE 33 Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

ARTICLE 34 Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

ARTICLE 35 Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment

may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demon-

strate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

ARTICLE 37 Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking

account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

ARTICLE 41 Monitoring of approved codes of conduct

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

2. A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:

(a) demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

(b) established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

(c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(d) demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The competent supervisory authority shall submit the draft criteria for accreditation of a body as referred to in paragraph

1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.

4. Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

5. The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the conditions for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.

6. This Article shall not apply to processing carried out by public authorities and bodies.

ARTICLE 42 Certification

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

3. The certification shall be voluntary and available via a process that is transparent.

4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.

5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the compe-

tent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.

6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

7. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.

8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

ARTICLE 49 Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

ARTICLE 83 General conditions for imposing administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of

the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12 to 22;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

(d) any obligations pursuant to Member State law adopted under Chapter IX;

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

ARTICLE 95 Relationship with Directive 2002/58/EC

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/E.

www.ddv.de