Datatilsynet
The Norwegian Data Protection Authority

CONSUMER AUTHORITY
NORWAY

DIGITAL SERVICES AND CONSUMER DATA

- The most important things you need to know about consumer and data protection as a developer, marketer, or provider of digital services

DATA-DRIVEN BUSINESS MODELS

Social media, mobile apps, search engines, online newspapers, personal assistants, GPS and map tools, and a number of other services are increasingly being offered without the consumer having to pay money to use them. Digital services where the business model entails making money from the consumer's personal data have become commonplace in the digital economy. Personal data is commercially valuable because it can be used to better understand consumer interests and patterns of behaviour.

However, the processing of personal data is subject to regulation. Both data protection laws and consumer protection laws limit what you can legally do.

Personal data means any information or inference that can be tied to a single individual, regardless of whether this information has been provided by the consumers themselves or registered through various tracking technologies. Personal data typically encompasses names, addresses, telephone numbers, e-mail addresses, national identity numbers and dynamic IP addresses. Information about patterns of behaviour is also considered personal data.

Examples of personal data include information about what consumers buy, which shops they patronise, which TV shows they watch, where they go and which websites they visit.

SCOPE

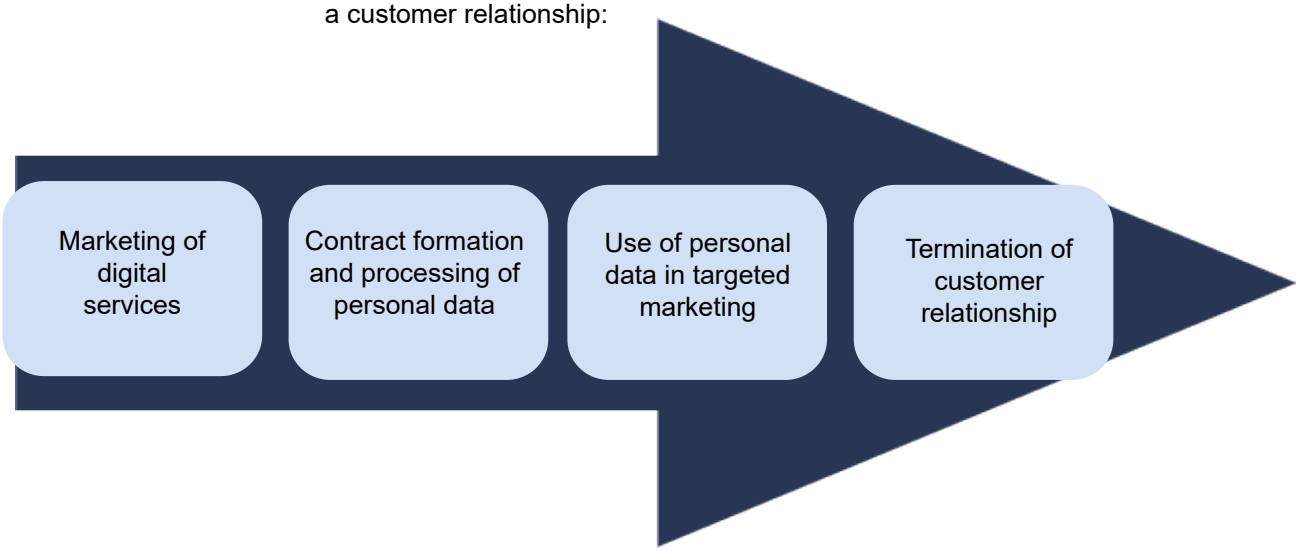
This guidance paper is part of the Norwegian Data Protection and Consumer Authorities' initiative to build knowledge and to guide businesses in practical situations where consumer and data protection overlap. As a provider of digital services to consumers, you must familiarise yourself with both of these fields of law, as they lay down important duties for digital services that process the personal data of consumers.

The guidance paper is intended as an introduction, and it is by no means exhaustive. It focuses on what information you must provide to consumers and the conditions for processing personal data. Many other relevant duties, such as the duty to implement data protection by design, the duty to ensure information security, and the duty to perform data protection impact assessments (DPIA) where necessary, will not be addressed here. It is nevertheless important that you familiarise yourself with these duties. There are also several exceptions from the main rules outlined below.

You will find more relevant information on **forbrukertilsynet.no** and **datatilsynet.no**. As concerns consumer protection law, some of the legal issues related to processing of personal data have not yet been fully clarified. This guidance paper expresses the Consumer Authority's preliminary position in these situations.

Compliance with the data protection rules described in this guidance paper is primarily the responsibility of the data controller, i.e. the party who determines the purposes and means of the processing of personal data. Compliance with consumer protection regulation is the responsibility of any party who markets or provides services to consumers. Violations of the data protection legislation may also be taken into account when the Consumer Authority considers a potential violation of the consumer protection legislation. That is why every link in the value chain should pay attention to both these sets of rules, regardless of whether they contribute directly or indirectly to any of the stages of the consumer relationship.

This guidance paper focuses on four stages — from marketing to the termination of a customer relationship:



MARKETING OF DIGITAL SERVICES

Consumers need clear and easily understandable information about the types of personal data your service collects, where you collect this personal data from and how you are using the personal data. Data protection legislation contains detailed requirements in this regard, put in place to ensure that consumers are informed when their personal data is being processed.

This information may also be important for consumers in deciding whether they want to use your service. How you process personal data may be such an integral part of the service that consumers must be provided with the most important aspects of this information in a clear and unambiguous way already at the marketing stage of your service. In these cases it is not sufficient for the information to be included in the terms of use or the privacy policy provided when users start using your service.

§ The Marketing Control Act prohibits unfair commercial practices, cf. Section 6. A commercial practice is always unfair and unlawful if it omits, hides or is otherwise likely to mislead the consumer about the main characteristics of the service, cf. Sections 7 and 8, cf. Section 6.

Remember:

- You should state in your marketing if your service is financed by the use of personal data, so that the consumer understands your business model.
  - *One example would be where you are using the consumer's personal data to target them with ads.*
- If your service processes personal data in a way that may have considerable impact on the consumer or that may come as a surprise, you should include information regarding this in your marketing.
  - *One example would be a map application that, uses location data to generate traffic statistics or visitor statistics for businesses, or a lifestyle app that shares activity data with third parties.*
- If your business model is to make money on the consumer's personal data, you should not market your services as "free" without also informing the consumer about this business model.
  - *One example would be a social media service that is free to use, but that is financed by using the consumers' personal data to target them with ads.*

- **Do not** market a function or feature of your service without informing consumers of the potential data protection impact.
  - *One example would be a service that generates bonus points for certain purchases, but requires that the consumer's purchase history is retained.*
- **Do not** market your services as "data protection friendly" or in similar turns of phrase without explaining to the consumer what you mean by this. You must be able to document all such claims.

CONTRACT FORMATION AND THE PROCESSING OF PERSONAL DATA

When the consumer decides to use your service, it is important to distinguish between

- the legal basis for processing, for example consent to the processing of personal data
- the terms and conditions for use of the service
- the privacy policy

Legal bases for processing

§ The rules concerning legal bases for processing follow from Article 5 (1) (a) and Article 6 GDPR, cf. Section 1 of the Personal Data Act. Article 4 (11), 7, and 8, and Recital 32 define what constitutes valid consent. The rules concerning processors primarily follow from Articles 28 and 29. The prohibition against processing special categories of personal data, as well as exceptions from this prohibition, follow from Article 9.

Virtually every service processes data about their users. In order to process personal data, you need a **legal basis for processing** pursuant to the Personal Data Act. The data controller must identify a suitable legal basis for each individual processing operation for each individual purpose, before the data is collected. collected.

This means that businesses are not free to use the terms and conditions of the contract to define how they will process personal data. For digital services, there are four legal bases for processing that are especially relevant: “necessary for the performance of a contract”, “necessary for compliance with a legal obligation”, “balancing of interests” or “consent”.

If you share personal data with others who do not exclusively process this data on your behalf, this processing requires its own basis for processing in order to be lawful. The sharing of personal data with others who exclusively process this data on your behalf, so-called data processors, is subject to **specific rules**.

Some personal data is so sensitive that the processing of this data is not permitted unless the person has given their explicit consent. For example, this applies to data concerning health, ethnic or racial background, religion or beliefs, political opinion and sexual orientation. **Read more.**

If the specified purpose can be achieved without processing personal data, the **data minimisation principle** states that the data cannot be collected.

The default settings of of a service can have considerable impact on how the service is used and how personal data are processed. The default settings must be the most data protection friendly, in line with the data protection principles.

Necessary for the performance of a contract

If the collection of personal data is objectively necessary to provide your service, the basis «**necessary for the performance of a contract**» may be suitable.

However, any processing of personal data that is not strictly necessary to provide the service, but is necessary to attain the commercial goals of your business, cannot be said to be “necessary for the performance of a contract”. Even if the terms and conditions specify that a specific type of processing of personal data is part of the service, this does not mean that this processing can

be based on “necessary for the performance of a contract”, if the processing is not actually and logically necessary to provide the service.

- *For example, a delivery address is necessary when ordering goods online, whereas the use of personal data to carry out profiling or develop data models is not necessary to provide a communications service. The processing of personal data to improve a service or develop new features can normally not be based on “necessary for the performance of a contract”.*

Necessary for compliance with a legal obligation

If you are obliged to process personal data under EU law or EEA Member State law, «**necessary for compliance with a legal obligation**» may be a relevant basis for your processing.

- *For example, it may be necessary to store some personal data to comply with statutory accounting obligations.*

Balancing of interests

The processing of personal data may be lawful if your **business’ legitimate interests outweigh the consumer’s interests, rights and freedoms, including the right to data protection.** However, if the data protection implications are not proportionate to the interest your business has in processing the data, your processing cannot be based on “balancing of interests”.

- *For example, a balancing of interest may be a suitable lawful basis for processing where your service monitors how often a consumer uses the service in order to prepare statistics for your own use and improve the service. On the other hand, a balancing of interest cannot be used to defend aggressive and detailed tracking or profiling for marketing purposes, because privacy considerations would override this interest.*

Consent

Processing of personal data can be based on **consent**. Consent must be the free and informed choice of the consumer. If consent is the lawful basis for your processing, you must make sure you ask for consent in the right manner.

Formation of contract and consent to the processing of personal data are two separate issues. Nevertheless, there seems be some confusion regarding this, both among businesses and consumers. Phrases like “By accepting these terms and conditions, you also consent to the processing of your personal data ...” are not uncommon, but nonetheless they are not in line with the law. It is important to know when to ask for consent and how to ask.

Remember:

- Make sure consent is freely given. The consumer should not experience any negative consequences or detriment if they do not give consent.
  - *For example, consent is not voluntary if the consumer cannot use a service unless they consent to tracking or profiling for marketing purposes.*
- Make sure the decision to give consent is informed, meaning that the consumer understands what they are consenting to and the consequences of doing so. For example,the consumer at least needs to know what types of personal data are being processed and for what purposes.
- Make sure the consent is specific and give the consumer the option of giving or withholding consent for each individual processing or purpose.
- Make sure the consumer gives consent through an affirmative action (opt in), e.g. by clicking a button or checking a box, and there can be no doubt that the consumer actually meant to give consent.

- Make sure the consent can be documented.
- Make sure the consent can be withdrawn as easily as it was to give.
- Make sure the request for consent is not mixed in with other information.
- Make sure the request for consent is not unnecessarily disruptive to the user experience.

- **Do not** combine terms and conditions for use with the request for consent.
- **Do not** bar the consumer from using your service if they do not consent to things that are not objectively necessary for the service.
- **Do not** bundle consent to different things in a non-granular manner.
- **Do not** use pre-checked boxes.
- **Do not** make it unnecessarily difficult or time-consuming to withhold consent, and do not use similarly aggressive means to influence or pressure the consumer into giving consent.
  - *Examples include the consumer having to decline the same processing several times or go through several extra steps to avoid giving consent.*
- **Do not** exaggerate the negative consequences for the consumer if they do not consent to the processing of personal data.

§ The duty to provide information about the processing of personal data follows from Article 5 (1) (a) and Articles 12–14 GDPR, cf. Section 1 of the Personal Data Act.

The Consumer Authority may prohibit unfair terms and conditions under Section 22 of the Marketing Control Act. In assessing what is unfair, emphasis is given to the balance between the parties' rights and obligations and to the clarity of the contractual relationship.

Terms and conditions and privacy policy

Terms and conditions are a contract that regulates rights and obligations between you and your users. You must make sure that they describe the service you provide and the relationship between you, your service and your users. There are certain statutory requirements as to what you must include in the terms and conditions. The terms and conditions must be clear, so that consumers can familiarise themselves with them and understand what they entail for them — including the processing of their personal data. In addition, terms and conditions must be balanced and not benefit you in such a way that it encroaches on the consumer's rights. See the **Consumer Authority's guidelines on digital terms and conditions**.

The privacy policy serves a different purpose than the terms and conditions and should instead **provide information about what the service does with the personal data it collects**, in accordance with the requirements of the Personal Data Act. This information should be provided no later than when the service begins to collect personal data from the consumers, and it must be provided separately from the terms and conditions and irrespective of which legal basis the processing is based on. The policy should, among other things, include information about which types of data are used for which purposes, what the legal basis for processing is and which rights the consumer has.

Remember

- Write your terms and conditions and your privacy policy in a straightforward, easily comprehensible way. This means you should strive to avoid legal jargon or specialist terminology not in common use.
- Make sure your terms and conditions are easily accessible, both at the time of contract formation and if the consumer wants to go back and read them later. The consumer should also be offered the option of saving the terms and conditions. Similarly, the privacy policy and information about the processing of personal data should be accessible both when the service collects data and later.
- Make sure the information most relevant to the consumer is highlighted in the terms and conditions and in the privacy policy, so that it is not hidden among all the other information. It may be a good idea to give a summary of the most important information at the top and use formatting, headings and a table of contents if this makes the terms and conditions and the privacy policy easier to understand.

- The privacy policy must be separate from the terms and conditions. **Learn more about what it must include here**. It may be a good idea to provide information in layers, so that the consumer can browse sub-layers to get more detailed information. This meets the legal requirement that the information must be both precise and brief, and makes it easier to highlight information of importance to the consumer.
- Clarify in your terms and conditions what the consumer's rights are if the protection of personal data is not in conformity with the contract. If the consumer has paid for use of the service, they should be entitled to have the service brought into conformity, a proportionate price reduction, termination of the contract, and, if relevant, compensation for financial loss, as in the case of other types of lack of conformity of services.
- If your business model is partly or entirely based on making money on the personal data of your users, you should make sure that this is made clear in your terms and conditions.

- **Do not** make your terms and conditions longer than they need to be. Terms and conditions that are excessively long quickly become difficult to follow. This makes it harder for the consumer to familiarise themselves with them and understand what they entail.
- **Do not** waive liability for the way in which third parties process personal data that you shared with them. You should exercise care with regard to who you share personal data with, if anyone.

§ The right to object to direct marketing, including targeted marketing, follows from Article 21, cf. Section 1 of the Personal Data Act. The rules for further processing of personal data for new purposes follow from Article 5 (1) (b) and Article 6 (4).

Targeted marketing may also be subject to Section 9, cf. Section 6, of the Marketing Control Act, which prohibits aggressive commercial practices. In determining whether a commercial practice is aggressive, account shall be taken of, among other factors, whether the trader is exploiting a specific misfortune or circumstance that is so serious that it may impair the consumer's judgement, to influence the consumer's decisions. Targeted marketing may also contravene good marketing practice, cf. Section 2 of the Marketing Control Act.

USE OF PERSONAL DATA IN TARGETED MARKETING

Personal data is often used in targeted marketing. By collecting and analysing personal data, it is possible to develop models for profiling, and consumers may be placed in the different profiles. Profiles may predict consumer preferences or mindsets. Commercial messages can then be adapted to the members of a given profile.

In order for you to be able to use information about your customers for profiling or marketing, you need a legal basis for processing, see above. This could, for example, be a valid consent or, if the profiles are only based on simple and non-intrusive characteristics such as age bracket and county of residence, a balancing of interests depending on the specific circumstances and interests. Profiling for marketing purposes can normally not be based on being "necessary for the performance of a contract". You also need a valid legal basis for processing even if you get your data from a third party, or if anyone else is assisting you in the profiling or marketing.

At the same time, you must also remember to inform consumers in a transparent way that you intend to use their data for profiling or marketing, see above.

Cookies and similar technologies are often used to collect data for use in profiling or marketing. Cookies are subject to the Electronic Communications Act, and the competent authority is the **Norwegian Communications Authority (NKOM)**. If personal data is collected with the help of cookies, the Personal Data Act applies in addition to the Electronic Communications Act, and this guide applies in its entirety for the subsequent processing.

If you use personal data for targeted marketing, you must be conscious of the types of data you collect, what the legitimate techniques for marketing persuasion are, and when you are approaching the limit of what constitutes undue and unlawful influence or pressure. This applies irrespective of the technology you use to target your advertising, and regardless of whether you use personal data or **properly anonymized data sets**.

A cookie is a small text file that is stored on the user's unit when the user opens a web page. Cookies are used for example to store login details, remember shopping baskets in online stores, or observe how the user navigates the website.

In addition, the Marketing Control Act includes specific requirements for marketing sent to the consumer via channels that allow for individual electronic communication, such as e-mails and text messages. Read more about this in the Consumer Authority's **guide to marketing via e-mail, text messages, etc.**

Remember:

- Make sure you have a legal basis for using personal data in targeted marketing.
- Make sure you inform the consumer adequately that you are collecting personal data for marketing purposes. In many instances, this is something the consumer will not expect, in which case this information must be highlighted.
- In your marketing, include clear information about how you processed the consumer's personal data to target them with this message.
- The consumer can at any time object to the use of their personal data **for direct or targeted marketing purposes**. You must clearly inform the consumer about this right, separate from any other information and at the latest at the time of the first communication with the consumer.

- **Do not reuse** personal data collected for a different purpose for profiling or targeted marketing, unless you obtain valid consent for such further processing.
- **Avoid** profiling or targeting that includes, predicts or deduces special categories of personal data, such as data concerning health, political opinion, ethnic or racial background, religion or beliefs or sexual orientation.
- **Do not** use personal data or other data concerning vulnerabilities or misfortunes and unfortunate circumstances for targeted marketing purposes.
    - *Examples of this includes information or inferences asserting that the consumer is having family problems, has low self-esteem, recently ended a relationship, has problems with gambling or compulsive shopping, or has difficulty paying their bills.*

TERMINATION OF CUSTOMER RELATIONSHIP

Data portability

The right to data portability grants to the consumer the right to receive personal data concerning them that they have provided to your service. The right to data portability is intended to make it easier for the consumer to switch between service providers or use several service providers simultaneously, thus preventing consumers from being locked in to a specific service or provider. The right to data portability only applies to data you have processed on the basis of consent or the data being "necessary for the performance of a contract". Furthermore, it must be data the consumer has actively provided to the service, or raw data on observed activity, such as logs and activity history. The right does not apply to refined data, such as your own analyses and profiles.

Remember:

- Provide information about the right to data portability in a clear, concise and easily accessible way.

§ The right to data portability follows from Article 20 GDPR, cf. Section 1 of the Personal Data Act. The rules on how to accommodate these rights, including rules concerning time limits and payment, follow from Article 12. The duty to ensure information security follows from Article 5 (1) (f) and Article 32.

- Make it easy for the consumer to exercise their right to data portability.
    - *For example, providers should facilitate for such requests to be made electronically.*
- If the conditions for data portability have been met, you must make this data available as soon as possible, normally within one month at the latest. If the conditions have not been met, you must notify the consumer of that within the same time limit.
- Make the data available in a structured, commonly used and machine-readable format, so that the data can be transferred to another service provider.
- If you deny the request for data portability, you should give your reasons for doing so, and at the same time provide information about the consumer's right to lodge a complaint with the Data Protection Authority.

- **Do not** charge a fee for complying with the request for data portability.
- **Do not** send the data without encryption, e.g. in an unencrypted e-mail.

Erasure of personal data

Your service has an obligation to facilitate the exercise of the consumer's data protection rights, such as **right to data erasure**. However, you also have an obligation to **consider erasure of your own initiative**. If your contractual relationship with the consumer is terminated, there will normally no longer be a basis for or need to process the consumer's personal data — the contract has been terminated and the purpose of processing the data has been achieved. It is prohibited to store personal data for longer than is necessary to achieve the purpose for which it was collected. This means that when this purpose has been achieved, the data shall be erased, even if the consumer has not requested it. In some cases, however, you may have a legal obligation to retain the information for a longer period of time, i.e. for compliance with the Accounting Act.

§ Provisions regarding erasure are found in Articles 5 (1) (e), 17, and 25 GDPR, cf. Section 1 of the Personal Data Act. The rules on how to accommodate these rights, including rules concerning time limits and payment, follow from Article 12

Remember:

- Provide information about the right to erasure in a clear, concise and easily accessible way.
- Make sure to have systems and procedures in place to ensure that your business automatically erases personal data if processing of that personal data is no longer necessary for the specified purpose.
- Erase data of your own accord if your processing is based on consent and the consumer withdraws consent, or if your processing is based on the performance of a contract and the contract is terminated, unless the data is simultaneously also processed for other purposes based on other legal bases.
- Make it easy for the consumer to exercise their right to erasure.
    - *For example, providers should facilitate for such requests to be made electronically.*
- If the conditions for erasure have been met, you must erase the data as soon as possible, normally within one month at the latest. If the conditions have not been met, you must notify the consumer of that within the same time limit
- If you deny the request for erasure, you must give your reasons for doing so, and at the same time provide information about the consumer's right to lodge a complaint with the Data Protection Authority.

- **Do not** charge a fee to erase the consumer's personal data.

CHILDREN AND YOUNG CONSUMERS

§ Marketing aimed at children must comply with the special provisions of the Marketing Control Act, cf. Chapter 4.

It follows from Recital 38 of the GDPR, cf. Section 1 of the Personal Data Act, that children merit specific protection with regard to their personal data, and especially in connection with marketing and profiling. The rules for children's consent with regard to information society services follow from Article 8 GDPR and Section 5 of the Personal Data Act.

Children and young people are vulnerable, and they are afforded special protection under both data protection and consumer law. They are generally less conscious of what processing of personal data entails, the risks involved, and which rights they have. They are also less experienced, more impressionable and easier to manipulate with commercial messages. It is very important that all services aimed at young people are especially mindful of the types of data they collect, how this data is used, how the data is protected and how these services provide information everyone can understand.

In principle, the term **children** means minors, i.e. all persons under the age of 18. However, in the Marketing Control Act, the term is applied with some flexibility. Age must be taken into account, and the younger a child is, the stricter any assessment pursuant to the Marketing Control Act will be.

If children and young people are profiled and pigeonholed, it may affect their ability to freely develop their unique identity. Profiling of children for marketing purposes should normally be avoided.

Remember:

- Adapt the information you provide when you ask children and young people for consent to process personal data, so that everyone can understand it.
- For information society services, such as most online services and apps, parents must consent to the processing of personal data on behalf of all children under the age of 13. In other contexts, 15 is normally the age limit for consenting to the processing of personal data. For sensitive personal data, such as data concerning health, political opinions, ethnic or racial background, religion or beliefs or sexual orientation, the age limit is always 18.

- **Do not** profile children for marketing purposes.
- **Do not** directly encourage children to buy something or to persuade their parents to buy it for them.

SUPERVISION AND SANCTIONS

Consumer protection legislation

The Consumer Authority seeks to exert influence on traders to comply with the Marketing Control Act, the Cancellation Act and other regulatory frameworks the Consumer Authority supervises. In case of violations of the Marketing Control Act or other consumer protection legislation, the Consumer Authority may decide to prohibit (Section 40), issue orders (Section 41), issue suspended penalties (Section 42) and in some cases impose administrative fines (Section 43), cf. Section 39 of the Marketing Control Act. Consumer Authority decisions may be appealed to the Market Council (Section 37).

Decisions may also be made concerning persons or businesses who are accessories to violations (Section 39, Subsection 2).

Data protection legislation

The Data Protection Authority is the supervisory authority pursuant to the Personal Data Act, and therefore it has the authority to request any information it deems necessary to verify compliance with the Act. If the provisions of the Personal Data Act or the GDPR are violated, the Data Protection Authority may issue warnings,

orders, reprimands, impose a ban on the processing of personal data or impose an administrative fine. This follows form Article 58 GDPR, cf. Section 1 of the Personal Data Act. If a controller does not comply with the Data Protection Authority's decision, the Authority may also impose a coercive fine pursuant to Section 29 of the Personal Data Act.

Depending on the circumstances of each individual case, and which provisions have been violated, the Data Protection Authority may impose an administrative fine of up to EUR 20 000 000 or 4 % of the total worldwide annual turnover of the preceding financial year. This follows from Article 83 GDPR, cf. Section 1 of the Personal Data Act.

In matters that concern consumers in multiple EEA states, there are specific provisions for how the data protection authorities in the different countries can work together in their supervisory activities.