NIEDERER KRAFT & FREY

Niederer Kraft & Frey Ltd
Bahnhofstrasse 13 · CH-8001 Zurich
Telephone +41 58 800 8000 · Telefax +41 58 800 8080
nkf@nkf.ch · www.nkf.ch

Breakfast Event – Data Protection Practical Tips

Dr. András Gurovits
Clara-Ann Gordon

8 February 2018

NKF

Die Bundesversammlung — Das Schweizer Parlament 04.02.2018

Freitag, 12. Januar 2018 11h00

MEDIENMITTEILUNG

REVISION DES DATENSCHUTZRECHTES IN ZWEI ETAPPEN

Die Notwendigkeit der vom Bundesrat vorgeschlagenen Anpassung des Datenschutzes an die gesellschaftlichen und technologischen Entwicklungen blieb in der Staatspolitischen Kommission (SPK) des Nationalrates unbestritten. Die Kommission möchte aber die Revision etappieren. Zuerst sollen die notwendigen Anpassungen an das europäische Recht vorgenommen werden. Die Totalrevision des Datenschutzgesetzes folgt in einer zweiten Etappe.

Die Staatspolitische Kommission (SPK) des Nationalrates ist ohne Gegenstimme auf die Vorlage des Bundesrates für die Totalrevision und die Änderung weiterer Erlasse zum Datenschutz (17.059) eingetreten. Gleichzeitig hat sie sich mit 14 zu 8 Stimmen bei 2 Enthaltungen für einen Ordnungsantrag ausgesprochen, welcher die Aufteilung der Vorlage vorsieht.

Die Teilung der Vorlage erlaubt es, die aufgrund der Schengen-Verträge innert einer bestimmten Frist notwendige Umsetzung von EU-Recht (Richtlinie 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten im Bereich des Strafrechts) vorab zu beraten. Anschliessend kann die Totalrevision des Datenschutzgesetzes ohne Zeitdruck angegangen werden. Auf diese Weise kann die Kommission der grossen Komplexität der Thematik gerecht werden. Eine Minderheit der Kommission lehnt die Teilung der Vorlage ab. Sie ist der Ansicht, dass zwei kurz aufeinander folgende Revisionen des Datenschutzgesetzes für die betroffenen Akteure zu Mehraufwand und Rechtsunsicherheit führen würden.

Die Kommission tagte am 11. Januar 2018 unter dem Vorsitz ihres Präsidenten Nationalrat Kurt Fluri (RL/SO) in Bern.

AUTOR

SPK-N
Sekretariat der Staatspolitischen Kommissionen
CH-3003 Bern
www.parlament.ch
spk.cip@parl.admin.ch

AUSKÜNFTE

Kurt Fluri
Kommissionspräsident
Tel. 079 415 58 88

Theres Kohler
Sekretariat SPK
Tel. 058 322 97 61

Revision des Datenschutzrechtes in zwei Etappen Seite 2 von 2
https://www.parlament.ch/press-releases/Pages/mm-spk-n-2018-01-12.aspx 04.02.2018

DIRECTIVES

DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16(2) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the Committee of the Regions [1],

Acting in accordance with the ordinary legislative procedure [2],

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union ('the Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Directive is intended to contribute to the accomplishment of an area of freedom, security and justice.

(3) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows personal data to be processed on an unprecedented scale in order to pursue activities such as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

(4) The free flow of personal data between competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security within the Union and the transfer of such personal data to third countries and international organisations, should be facilitated while ensuring a high level of protection of personal data. Those developments require the building of a strong and more coherent framework for the protection of personal data in the Union, backed by strong enforcement.

(5) Directive 95/46/EC of the European Parliament and of the Council [3] applies to all processing of personal data in Member States in both the public and the private sectors. However, it does not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as activities in the areas of judicial cooperation in criminal matters and police cooperation.

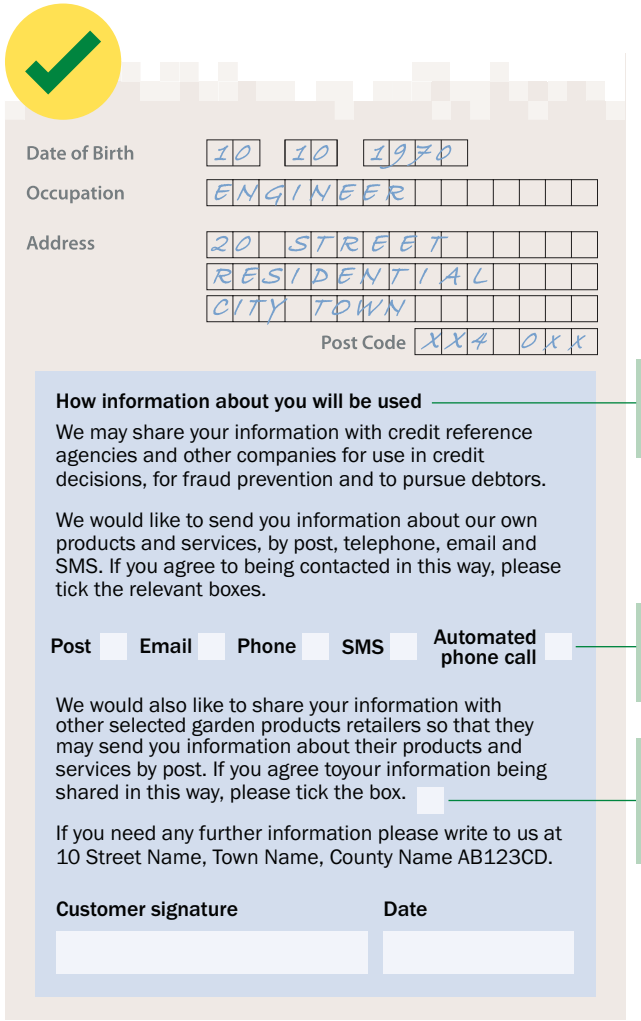
[1] OJ C 391, 18.12.2012, p. 127.
[2] Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April 2016.
[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

Data Privacy Notice – Checklist

- What?
  - (i) Identity and contact details of the controller and where applicable, the controller's representative and the data protection officer.
  - (ii) Purpose of the processing and the lawful basis for the processing.
  - (iii) The legitimate interests of the controller or third party, where applicable.
  - (iv) Categories of personal data.
  - (v) Any recipient or categories of recipients of the personal data.
  - (vi) Details of transfers to third country and safeguards.
  - (vii) Retention period or criteria used to determine the retention period.
  - (viii) The existence of each of data subject's rights.
  - (ix) The right to withdraw consent at any time, where relevant.
  - (x) The right to lodge a complaint with a supervisory authority.
  - (xi) The source the personal data originates from and whether it came from publicly accessible sources.
  - (xii) Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data.
  - (xiii) The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.
- Form?
  - (i) orally,
  - (ii) in writing,
  - (iii) through signage, and
  - (iv) electronically.
- When?
  - (i) At the time when information is obtained.
  - (ii) No information is necessary where data subject already has information.
  - (iii) At any time actively if:
    - sensitive information is being collected,
    - intended use of the information is likely to be unexpected or objectionable,
    - providing personal information, or failing to do so, will have a significant effect on the data subject, or
    - the information will be shared with another organisation in a way that data subjects would not expect.
- How?

  Information must be written and presented effectively by:
  - (i) using clear, straightforward language,
  - (ii) adopting a style that the audience will understand,
  - (iii) not assuming that data subject has the same level of understanding,
  - (iv) avoiding confusing terminology or legalistic language,
  - (v) aligning to the house style,
  - (vi) aligning with the organisation's values and principles,
  - (vii) being truthful and not offering data subjects choices that are counter-intuitive or misleading,
  - (viii) following any specific sectoral rules,
  - (ix) ensuring all notices are consistent and can be updated rapidly, and
  - (x) providing separate notices for different audiences.

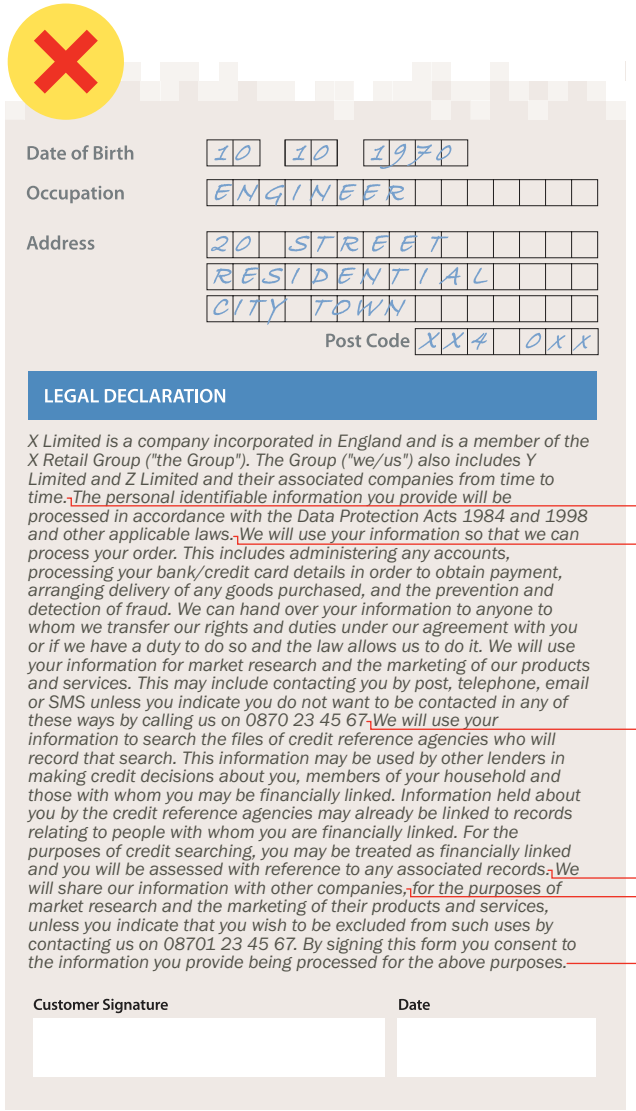
Quelle: https://ico.org.uk/media/for-organisations/documents/1625136/good-and-bad-examples-of-privacy-notices.pdf



Simple language, clear font and style.

Clear opportunity to agree to marketing.

Prior consent sought for postal marketing by other companies.



Confusing and legalistic language. Closely spaced text, small italic font in light grey.

Unnecessary – means little to the public.

Specific opt-in consent is required for some e-marketing and is good practice for all direct marketing.

Confusing language.

No details of what type of companies.

Bad practice to seek one consent for several types of processing.

Please provide telephone numbers in case we need to contact you about your claim.

You do not have to tell us your phone number but it will help us to contact you quickly if we have a question about your claim.

Home:	Mobile:

Clear explanation of why it would be helpful to provide this information.

About your claim - Sharing information

Sharing information with your landlord could help us to deal with your claim more quickly and reduce the risk of you falling behind with your rent because of your claim being delayed.

If your housing benefit is paid directly to your landlord or to your council rent account, then we can discuss payment details (eg award dates and amounts) as we have to give your landlord this information.

With your permission, we would also be able to tell your landlord if:

- You have claimed housing benefit
- We have made a decision on your claim, or
- We need more information to make a decision and what that information is.
- You can withdraw your permission at any time.
- We won't give your landlord any information about:
- Your personal or family circumstances.

Your finances

It will not affect your claim if you do not give us permission to discuss your claim with your landlord.

If we can talk to your landlord about your claim please sign below.

I give my local council permission to share information about the progress of my housing benefit claim with my landlord or their representative.

Signature of claimant:	Date:
Signature of partner:	Date:

Honest explaination of the outcome of choosing not to provide the requested information.

Your declaration

I understand the following:

You will use the information I have provided to process my claim for housing benefit, council tax benefit, or both.

You may check some of the information with other sources within the council, the rent service, other councils and government departments, eg the benefits agency, the Inland Revenue and the Home Office.

You may also get information about me from certain other organisations, or give information about me to them to: make sure the information is accurate; prevent or detect crime; and protect public funds. These other organisations include government departments, other local authorities and private sector organisations such as banks and organisations that may lend me money.

If I give information that is incorrect or incomplete you may take action against me, including court action.

I declare that the information I have given on this form is correct and complete.

Signature of the person claiming:

Clear explanation of purpose and use.

You must provide the following telephone numbers. It will delay your claim if you don't provide your telephone numbers.

Home: **Mobile:**

Implies it is mandatory to give this information when in this case it is voluntary.

About your claim - Sharing information

Enabling us to share your personal data with your landlord and other third parties could help us to deal with your claim more quickly and reduce the risk of any delay with the processing of your claim which may cause you to fall into arrears with your rental payment.

If your Housing Benefit is paid directly to your landlord or to your Council rent account, then we can discuss payment details (eg award dates and amounts) as we have to give your landlord this information. However, if you sign below we would also be able to tell your landlord whether you have claimed Housing Benefit or we have made a decision on your claim, or we need further information to make a decision about your claim and what that information may be.

Signature of claimant: Date:

Signature of partner: Date:

By signing above you agree that we can share information about the progress of your Housing Benefit claim with your landlord /landlady or their representative.

It will not affect your claim if you don't give us permission to discuss your claim with your landlord.

This should appear before the signature box, so that individuals are fully aware of the choice to provide or not to provide the information.

Doesn't say who the other third parties are.

Declaration

I hereby confirm my understanding of and acceptance of the following information. Donningly Council (the 'Council') will utilise the personal data I have provided in this form and via any evidence I have submitted in support of my claim in order to process my claim for housing benefit, council tax benefit, both of these or other applicable benefits which may be available to myself in accordance with the Council's personal data usage policies. The Council may check the personal data against other sources within the Council and other relevant third party public sector organisations as necessary in order to prevent and detect crime, protect public funds and make sure the personal information is accurate. The Council may also require to check personal data I have provided, or information in relation to myself, which has been provided to the Council by a third party with other information held by the Council. The Council may also get information about me from third parties or give information about me in accordance with the law. For the purposes of the Data Protection Act 1998 the data controller processing your personal data is Donningly Council. The Council processes all personal data in accordance with the Data Protection Act 1998 and the law.

Having read and understood the above information I hereby provide declaration that the data on this form is correct and comprehensive and understand that if I give the Council information that is incorrect or incomplete the Council may commence legal action against me potentially leading to or including court action.

Signature:

Confusing language.

not be due and payable immediately and will not be attached to the terms of any default notice issued by you.

Using your personal information

6. Personal information which you supply to us may be used in a number of ways, for example:

- To make lending decisions
- For fraud prevention
- For audit and debt collection
- For statistical analysis

(i) We may share your information with, and obtain information about you from, credit reference agencies or fraud prevention agencies, If you apply to us for insurance we will pass your details to the insurer. Information provided by you may be put onto a register of claims and shared with other insurers to prevent fraudulent claims.

(ii) We will not disclose any information to any company outside the XXXX Bank Group except to help prevent fraud, or if required to do so by law

(iii) For further information on how your information is used, how we maintain the security of your information , and your rights to access information we hold on you, please contact: (clear web link/freephone etc.)

Title that people will understand.

Clarity about who personal information is shared with and why.

Clear info about how to find out more. Easy, free access.

not be due and payable immediately and will not be attached to the terms of any default notice issued by you.

DPA Statement

6. I/we agree that You and any lender resulting from this application (the" Lender") shall be entitled to use and process, by any medium, the information given by me/us which may be acquired during the lifetime of any loan for the following purposes:

(i) to provide data and search the files of credit reference agencies or fraud prevention agencies whether before or during the lifetime of any loan granted me/us by the Lender

(ii) to disclose the data to credit reference agencies when required by them for future applications for finance by me/us or my/our financial associates unless I/we successfully file a disassociation with the credit reference agencies.

(iii) to disclose the data to any other company within the XXXX Bank Group or to any third party at any time for the purpose of assessing my/our application and administering and enforcing any subsequent loan

(iv) to disclose the data to any third party who replaces my/our Lender.

By submitting your personal data you CONSENT to it being processed.

We will share information about you within the XXXX Bank Group and also with other selected companies to provide you with information about products/services which we believe may be of interest to you.

Under the terms of the Data Protection Act 1998 you have the right to make a subject access request. All requests must be made in writing to our head office. There is a charge for this service.

If you do not wish to receive marketing information from XXXX Bank Group or other companies please inform your branch.

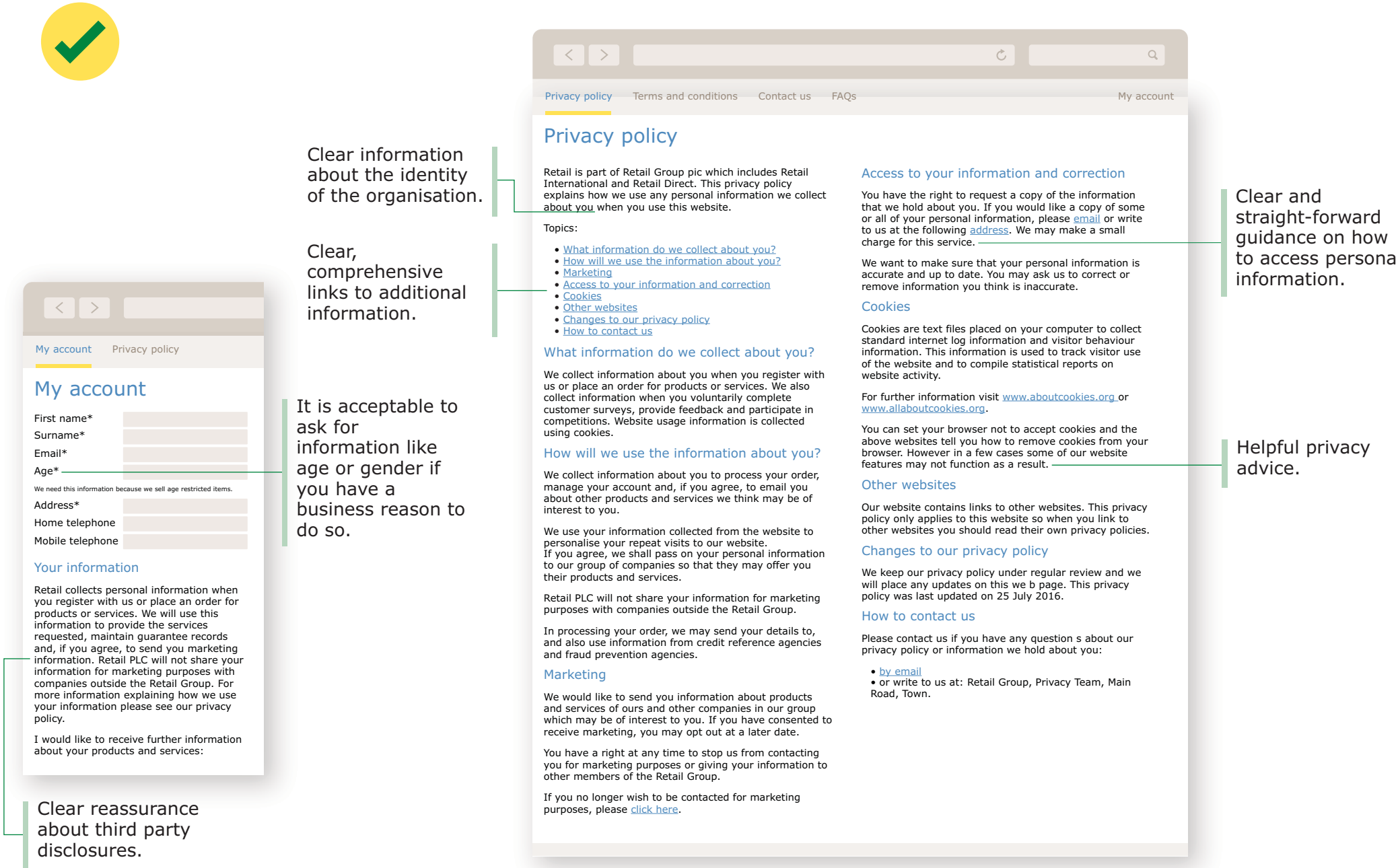
Title doesn't mean much to the public.

Unnecessarily complicated language. Use of I or me, we or us etc adds to confusion.

Doesn't describe the companies sufficiently or say how they will provide this marketing information.

Unclear, offputting notice – seems like a difficult, expensive process. People may not know what a subject access request is.

Small print, not easy to do (i.e. contact branch). Opt-out statement not next to statement about marketing information.


Clear information about the identity of the organisation.
Clear, comprehensive links to additional information.
It is acceptable to ask for information like age or gender if you have a business reason to do so.
Clear reassurance about third party disclosures.
Clear and straight-forward guidance on how to access personal information.
Helpful privacy advice.
My account
Privacy policy
Terms and conditions
Contact us
FAQs
My account
Privacy policy
Retail is part of Retail Group pic which includes Retail International and Retail Direct. This privacy policy explains how we use any personal information we collect about you when you use this website.
Topics:
What information do we collect about you?
How will we use the information about you?
Marketing
Access to your information and correction
Cookies
Other websites
Changes to our privacy policy
How to contact us
What information do we collect about you?
We collect information about you when you register with us or place an order for products or services. We also collect information when you voluntarily complete customer surveys, provide feedback and participate in competitions. Website usage information is collected using cookies.
How will we use the information about you?
We collect information about you to process your order, manage your account and, if you agree, to email you about other products and services we think may be of interest to you.
We use your information collected from the website to personalise your repeat visits to our website.
If you agree, we shall pass on your personal information to our group of companies so that they may offer you their products and services.
Retail PLC will not share your information for marketing purposes with companies outside the Retail Group.
In processing your order, we may send your details to, and also use information from credit reference agencies and fraud prevention agencies.
Marketing
We would like to send you information about products and services of ours and other companies in our group which may be of interest to you. If you have consented to receive marketing, you may opt out at a later date.
You have a right at any time to stop us from contacting you for marketing purposes or giving your information to other members of the Retail Group.
If you no longer wish to be contacted for marketing purposes, please click here.
Access to your information and correction
You have the right to request a copy of the information that we hold about you. If you would like a copy of some or all of your personal information, please email or write to us at the following address. We may make a small charge for this service.
We want to make sure that your personal information is accurate and up to date. You may ask us to correct or remove information you think is inaccurate.
Cookies
Cookies are text files placed on your computer to collect standard internet log information and visitor behaviour information. This information is used to track visitor use of the website and to compile statistical reports on website activity.
For further information visit www.aboutcookies.org or www.allaboutcookies.org.
You can set your browser not to accept cookies and the above websites tell you how to remove cookies from your browser. However in a few cases some of our website features may not function as a result.
Other websites
Our website contains links to other websites. This privacy policy only applies to this website so when you link to other websites you should read their own privacy policies.
Changes to our privacy policy
We keep our privacy policy under regular review and we will place any updates on this we b page. This privacy policy was last updated on 25 July 2016.
How to contact us
Please contact us if you have any question s about our privacy policy or information we hold about you:
by email
or write to us at: Retail Group, Privacy Team, Main Road, Town.
My account
Privacy policy
My account
First name*
Surname*
Email*
Age*
We need this information because we sell age restricted items.
Address*
Home telephone
Mobile telephone
Your information
Retail collects personal information when you register with us or place an order for products or services. We will use this information to provide the services requested, maintain guarantee records and, if you agree, to send you marketing information. Retail PLC will not share your information for marketing purposes with companies outside the Retail Group. For more information explaining how we use your information please see our privacy policy.
I would like to receive further information about your products and services:

RETAIL ACCESSORIES™

Select country £

Log in

Your details

First name*

Surname*

Email*

Date of birth*

Address*

Home phone number*

Mobile phone number*

Profession*

Salary*

Fields marked * are mandatory

By using this website I agree to the Retail terms and conditions.

ACCEPT

Retail Group Terms and Conditions

1. This website is owned and operated by Retail Group Ltd in conjunction with its subsidiaries XYXY Inc and BAAB Company. All orders and purchases made through this website are subject to these online shopping terms and conditions.

2. Retail Group may without notice correct errors and update information on this website. This may include information on pricing and availability of stock. All prices listed on this website are in pounds sterling and all charges will be processed in this currency.

3. Purchases made on this website, the use of this website and these online retail terms and conditions are subject to the laws of the United Kingdom.

4. Goods may only be purchased for lawful, non-commercial purposes. In ordering items, you agree to pay for all charges applicable on that purchase order as stated.

5. Only persons aged 18 or over may purchase from this website. Items purchased cannot be delivered to addresses outside the United Kingdom.

6. Retail Group Limited including its subsidiaries, associates and affiliated companies ("we'; "us") take security of information very seriously and are committed to protecting your privacy.

7. By using this website you accept the conditions set out in this privacy policy.

8. We process personal data in accordance with the Data Protection Acts of 1984 and 1998 and any other applicable legislation (referred to as the "data protection legislation").

9. We can assure you that we will never pass on the personal data of data subjects to any third party recipients other than in accordance with the Terms set out below.

10. We may collect and process personal data for the purposes of business operations. This could include: administration, accounting and auditing, processing of your order, marketing, analysis, monitoring, business planning etc, in accordance with the notification requirements of the Information Commissioner. We are registered with the Information Commissioner's Office. Members of the Retail Group may record, use, exchange, analyse and assess any relevant personal data.

11. We adhere to the Principles of data protection as set out in the Data Protection Act 1998 and observe the conditions relating to the fair and lawful processing of personal data. We may from time to time send you details of goods and services, new products, special offers, competitions which we think will be of interest to you.

12. By using this website you agree to the disclosure of collected personal data to carefully selected third party recipients for the purposes of advertising, marketing and public relations.

13. Information held by the credit reference agencies is used by us and others to help verify the identity of customers and assess their ability to meet financial commitments. Credit reference agencies may link the records of financial associates who have entered into joint financial obligations. Once linked this association means that each record will be taken into account when assessed by us. Further details about financial association, disassociation and credit reference agencies are available by contacting the credit reference agencies directly.

14. We shall process personal data that is considered to be "sensitive personal data" only in accordance with the requirements of the data protection legislation.

15. Should you wish to exercise your subject access rights as set out in data protection legislation, please contact us on 087 [premium phone number] ... for details of fees and a copy of our data subject access rights procedure. It is a legal requirement of the Data Protection Act 1998 that such requests must be made in writing.

Privacy policy is buried in the terms and conditions.

Misleading guarantee that your information will never be shared.

No opportunity to opt out in or out of receiving marketing.

Unhelpful not to provide contact details.

Subject access is made to sound like a difficult, legalistic and expensive process.

ARTICLE 29 DATA PROTECTION WORKING PARTY

00264/10/EN
WP 169

Opinion 1/2010 on the concepts of "controller" and "processor"

Adopted on 16 February 2010

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate D (Fundamental Rights and Citizenship) of the European Commission, Directorate General Justice, Freedom and Security, B-1049 Brussels, Belgium, Office No LX-46 01/190.

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

Executive summary

The concept of data controller and its interaction with the concept of data processor play a crucial role in the application of Directive 95/46/EC, since they determine who shall be responsible for compliance with data protection rules, how data subjects can exercise their rights, which is the applicable national law and how effective Data Protection Authorities can operate.

Organisational differentiation in the public and in the private sector, the development of ICT as well as the globalisation of data processing, increase complexity in the way personal data are processed and call for clarifications of these concepts, in order to ensure effective application and compliance in practice.

The concept of controller is autonomous, in the sense that it should be interpreted mainly according to Community data protection law, and functional, in the sense that it is intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis.

The definition in the Directive contains three main building blocks:
- the personal aspect ("*the natural or legal person, public authority, agency or any other body*");
- the possibility of pluralistic control ("*which alone or jointly with others*"); and
- the essential elements to distinguish the controller from other actors ("*determines the purposes and the means of the processing of personal data*").

The analysis of these building blocks leads to a number of conclusions that have been summarized in paragraph IV of the opinion.

This opinion also analyzes the concept of processor, the existence of which depends on a decision taken by the controller, who can decide either to process data within his organization or to delegate all or part of the processing activities to an external organization. Two basic conditions for qualifying as processor are on the one hand being a separate legal entity with respect to the controller and on the other hand processing personal data on his behalf.

The Working Party recognises the difficulties in applying the definitions of the Directive in a complex environment, where many scenarios can be foreseen involving controllers and processors, alone or jointly, with different degrees of autonomy and responsibility.

In its analysis, it has emphasized the need to allocate responsibility in such a way that compliance with data protection rules will be sufficiently ensured in practice. However, it has not found any reason to think that the current distinction between controllers and processors would no longer be relevant and workable in that perspective.

The Working Party therefore hopes that the explanations given in this opinion, illustrated with specific examples taken from the daily experience of data protection authorities, will contribute to effective guidance on the way to interpret these core definitions of the Directive.

Anhang
(Ziff. I)

Bundesgesetz über den Datenschutz
(Datenschutzgesetz, DSG)

Entwurf

vom …

Die Bundesversammlung der Schweizerischen Eidgenossenschaft,
gestützt auf die Artikel 95 Absatz 1, 97 Absatz 1, 122 Absatz 1 und 173 Absatz 2 der Bundesverfassung[20],
nach Einsicht in die Botschaft des Bundesrates vom 15. September 2017[21],
beschliesst:

1. Kapitel: Zweck und Geltungsbereich sowie Aufsichtsbehörde des Bundes

Art. 1 Zweck

Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Personendaten bearbeitet werden.

Art. 2 Geltungsbereich

[1] Dieses Gesetz gilt für die Bearbeitung von Personendaten natürlicher Personen durch:

a. private Personen;

b. Bundesorgane.

[2] Es ist nicht anwendbar auf:

a. Personendaten, die von einer natürlichen Person ausschliesslich zum persönlichen Gebrauch bearbeitet werden;

b. Personendaten, die von den eidgenössischen Räten und den parlamentarischen Kommissionen im Rahmen ihrer Beratungen bearbeitet werden;

[20] SR **101**
[21] BBl **2017** 6941

Art. 8 Bearbeitung durch Auftragsbearbeiter

[1] Die Bearbeitung von Personendaten kann vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden, wenn:

a. die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und

b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

[2] Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftrag sbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.

[3] Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen.

[4] Er kann dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche.

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee ([1]),

Having regard to the opinion of the Committee of the Regions ([2]),

Acting in accordance with the ordinary legislative procedure ([3]),

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

(3) Directive 95/46/EC of the European Parliament and of the Council ([4]) seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

([1]) OJ C 229, 31.7.2012, p. 90.
([2]) OJ C 391, 18.12.2012, p. 127.
([3]) Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April 2016.
([4]) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

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.

Structure of data processor agreement

- Parties, introduction.
- Details about the processing, such as:
  - (i) the subject matter and duration of the processing,
  - (ii) the scope, nature and purpose of the processing,
  - (iii) the type of personal data processed and the categories of data subjects,
  - (iv) obligations and rights of the data controller.
- Obligations of the data processor:
  - (i) Obligation of the processor to process personal data only on documented instructions from the controller including with regards to cross-border data transfers.
  - (ii) Obligation of the processor to impose confidentiality obligations on all personnel authorized to/engaged for processing of the personal data.
  - (iii) Obligation of the processor to assist the controller in ensuring compliance with the data security requirements; and obligation of the processor to ensure the security of any personal data being processed (cf. article 32 GDPR).
  - (iv) Obligation of the processor in respect of sub-processors, in particular:
    - obligation not to use another processor without the controller's authorisation,
    - obligation of the processor to inform of any changes made in its relationship with a permitted sub-processor,
    - the processor's obligation to impose on the sub-processor all contract terms required in accordance with article 28 para. 3 of the GDPR, and
    - obligation of the processor to remain liable even if it has sub-contracted to a sub-processor.
  - (v) Obligation of the processor to assist controller in meeting its obligations vis-à-vis data subjects, i.e. that they can exercise their rights for
    - access,
    - rectification or erasure, and
    - making objections to the processing.
  - (vi) Obligation of the controller, taking into account the nature of the processing and information available to the processor, to:
    - assist the controller in meeting its obligations in accordance with article 32 of the GDPR to keep the personal data secure,
    - assist the controller in meeting its obligations in accordance with article 33 of the GDPR to notify personal data breaches,
    - assist the controller in meeting its obligations in accordance with article 34 of the GDPR to advise data subjects when there has been a personal data breach,
    - assist the controller in meeting its obligations in accordance with article 35 of the GDPR to carry out data protection impact assessments (DPIAs), and
    - assist the controller in meeting its obligations in accordance with article 36 of the GDPR to consult with the supervisory authority where the DPIA indicates there is an unmitigated risk to the processing.
  - (vii) Obligation of the processor to, at the controller's election, either return or destroy the personal data at the end of the relationship (unless the law would require a longer retention period).
  - (viii) Obligation in respect of audits and inspections, in particular, obligation of the processor to:
    - provide the controller with all information required to demonstrate that both, the controller and the processor, meet the requirements under article 28 GDPR,
    - contribute to audits and inspections that the controller wants to carry out or that a third party auditor shall carry out on behalf of the controller,
    - inform the controller without delay if it believes that instructions given do not comply with the GDPR.

Further considerations

- The GDPR allows use of standard contract terms issued by the EU Commission or a supervisory authority (to our knowledge, however, no such terms are available yet).
- The GDPR also allows these standard terms to form part of a code of conduct (to our knowledge, however, no such codes are available yet).
- Only use processors that are able to ensure to fulfil the requirements of the GDPR, i.e. carefully select the processor, and do not use its services before a written contract that is article 28-compliant has been executed.
- Responsibilities of the processor, by operation of law, include:

  (i) to only act on the basis of documented instructions,

  (ii) to not use sub-processors without prior written authorisation of controller,

  (iii) to co-operate with the supervisory authority,

  (iv) to ensure the security of its processing,

  (v) to keep records of the processing activities,

  (vi) to notify any personal data breach to the controller,

  (vii) to appoint a representative in the EU if needed.

- If processor fails to meet these obligations it can be subject to fines or other corrective measures by the supervisory authority.