

Bristows

Responding to data subject requests

Robert Bond robert.bond@bristows.com



1

Robert Bond – Partner, Commercial/IP/IT

Robert Bond has over 40 years' experience in advising national and international clients on all of their technology, data protection and information security law requirements. He is a recognised legal expert and author in the fields of IT, e-commerce, computer games, media and publishing, data protection, information security and cyber risks.

Robert is Listed in Legal 500 as a Leading Individual for Data Protection where he is described as "astounding" and in Band 1 for Data Protection in Chambers UK 2019 where clients describe him as "absolutely exemplary" and the fact that his knowledge of data protection law is "astounding, and his application equally impressive."

Robert is 2nd VP of the Board of the Society for Corporate Compliance & Ethics, Chairman of the Data Protection Network, Trustee of the UK Safer Internet Centre, a member of the Data Privacy Advisory Group to the United Nations and an Ambassador for Privacy by Design.



Robert Bond

2

2

Established in 1837, Bristows has always been associated with top-tier, full-service legal work involving innovative clients. Today we remain an independent, international law firm bringing together a diverse collection of talent to deliver high-quality legal advice and service.



3

Topics

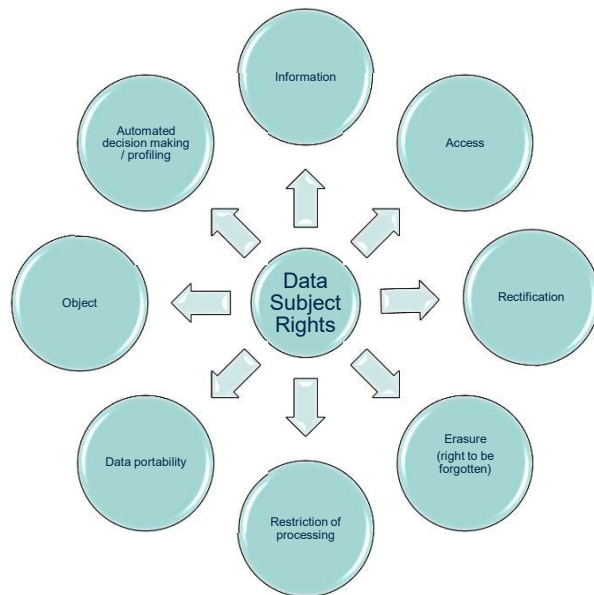
- Overview of EU data subject requests
- Subject Access Requests (DSARs)
- Portability
- Erasure



4

Data subjects rights

5



5

Access

6

Controllers must provide the data subject with information on action taken on a request **without undue delay** and, at the latest within **one month** of receipt of the request

May be **extended** for a maximum of **two months** when necessary, taking in to account:

- the complexity of the request; and
- the number of requests.

Information and actions relating to data subjects rights

– **free** of charge unless request is **manifestly unfounded** or **excessive / repetitive**, in which case the controller may charge a reasonable fee for administrative costs



6

What is a subject access request?

7

Used most often used by individuals who want to see a **copy** of the information an organisation holds about them

Common misconception: SAR is a right to obtain a **copy** of personal information, it is **NOT** a right to documentation!!

But that is not all... individuals are also entitled to be:

1. told whether any personal data is being processed;
2. given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
3. given a copy of the information comprising the data; and given details of the source of the data (where this is available).

7

Procedure – first steps

- Identify the request
- Log and report internally
- Check formalities
- Check identity and authority
- Acknowledge receipt and request fee/other info?
- Diarise deadline

8

Formalities



The controller may require additional information

- validate identity (what do you *reasonably* require?)
- locate requested information (do you know where to look for it?)

Timescale for responding: promptly, within 30 days

May be extended for a further two months *when necessary*, taking into account complexity and number of requests

9

Other considerations



- Data held at the time the request received – do not change/delete
- Repeat requests:
 - Identical or similar request
 - “reasonable” interval.

May refuse to act on requests if *manifestly* unfounded or excessive, e.g. because repetitive

10

Procedure – next steps

- Leave enough time to locate data and prepare response!
- Set search parameters and undertake search
- Exclude some information? (e.g. third party data or exemptions)
- Prepare copies ready for disclosure
- Prepare other information (e.g. purposes, recipients, sources, explanations)
- Disclose the relevant information to the data subject (30 days)
- Keep a record of decisions made and information sent

11

Search criteria

Electronic systems

- Network and local storage (by different teams/staff members)
- Wider than just main databases, e.g. communications (emails, SMS, IMs, social media...?)
- Backups, archives

Manual files

- Relevant filing systems, e.g. personnel files, complaint files
- Unstructured paper records for public authorities

Involve others

- Your staff
- Processors

12

Search criteria

Search locations

- Locations which you (or your staff) know may contain personal data
- Locations identified by the data subject
- General search for general request; specific search for specific request

Search terms

- Name & variations , e.g. Robert Bond, R.Bond, RTJBond
- Other identifying info, e.g. images, customer/staff number
- Other info provided by the data subject, e.g. dates, other individuals

Maintain logs and audit trails

13

Search criteria

Decide which data to provide

- Is it all 'personal' data?
- Are you happy to provide all of it?
- Is it within the scope of the request?
- Data which reveals the identity of another person: can it/should it be excluded?
- Data to which an exemption to access applies

Data not documents

- Redact documents; or
- Extract data from documents
- No need to provide same data twice

14

How should the information be provided?

- **Intelligible form:**
 - understood by average person
 - explain complex/technical terms or codes (e.g. database acronyms)
- **Permanent form** unless:
 - data subject agrees otherwise; or
 - disproportionate effort (but must still allow access)

Also consider security



15

What is a subject access request?

1
6

SUBJECT ACCESS REQUEST - [NAME OF THE DATA SUBJECT]

Personal data	Purposes	Recipients / class of recipients	Source of the personal data	Date
[example - Joe Bloggs was on sick leave for two weeks]	[example - for staff administration purposes]	[example - workplace healthcare provider, counterparties, credit reference agency]	[example - Joe Bloggs' data subject himself]	

16

Exemption – management forecasting

- Management forecasting or planning
- In the conduct of any business or activity (includes public sector)
- Exempt from SARs to the extent **likely to prejudice** the conduct of that business or activity

Consider: existing and past information – does it still prejudice?

Example: planned redundancies or changes to staffing

17

Exemption – negotiations

- Records of the intentions of the data controller
- In relation to any negotiations with the data subject
- Exempt to the extent **likely to prejudice** those negotiations
- Less likely to apply once the negotiations are concluded

18

Exemption – legal professional privilege

- Data in respect of which a claim to legal professional privilege could be maintained in legal proceedings
- “Privilege” is interpreted in case law; scope may be narrower than you think:
 - Legal advice privilege
 - Litigation privilege
- External or in-house lawyers, *but* communication must be for legal advice or litigation (not merely cc’ing into wider discussions)

19

Exemption – confidential references

- **A reference given or to be given in confidence:** education, employment, provision of service



20

Exemption – prevention or detection of crime

Exempt to the extent to which **likely to prejudice:**

- prevention or detection of crime
- apprehension or prosecution of offenders
- assessment or collection of any tax or duty

Example: suspected criminal activity and communications with the police

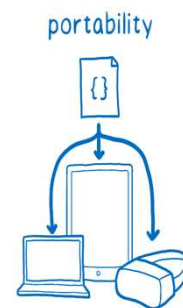
Consider: current and past investigations

21

Portability

- Individuals can obtain and reuse their personal data for their own purposes across different services
- They can move, copy or transfer personal data from one IT environment to another in a safe and secure way, without affecting its usability
- This may enable them to take advantage of applications and services that can use this data to find a better deal or help them understand their spending habits
- The right only applies to information an individual has provided to a controller
- It only applies where the information was processed on the lawful grounds of consent or contract performance

✓ So develop a procedure and plan for responding to a Data Portability request



2
2

22

Erasure

- Individuals can request for erasure of their personal data – also known as “the right to be forgotten”
- They can make the request verbally or in writing
- Erasure applies in most circumstances including back-ups
- You do not have to erase if you are required to keep the data by law or for public tasks or archiving or defence of claims
- You need to cross reference your data retention policy

✓ So develop a procedure and plan for responding to a Data Erasure request



23

Example SAR

Dear Sir or Madam

Subject access request

[Your full name and address and any other details to help identify you and the data you want.]

Please supply the data about me that I am entitled to under data protection law relating to: [give specific details of the data you want, for example:

- my personnel file
- emails between 'person A' and 'person B' (from 1 June 2017 to 1 Sept 2017)
- my medical records (between 2014 and 2017) held by 'Dr C' at 'hospital D'
- CCTV camera situated at ('location E') on 23 May 2017 between 11am and 5pm
- copies of statements (between 2013 and 2017) held in account number xxxxx.]

If you need any more data from me, or a fee, please let me know as soon as possible. It may be helpful for you to know that data protection law requires you to respond to a request for data within one calendar month.

If you do not normally deal with these requests, please pass this letter to your DataProtection Officer, or relevant staff member. If you need advice on dealing with this request, the Information Commissioner's Office can assist you. Its website is ico.org.uk or it can be contacted on 0303 123 1113.

Yours faithfully

bristows.com

24

Questions?



25

Thank you

Bristows LLP
100 Victoria Embankment
London EC4Y 0DH
T +44 20 7400 8000

robert.bond@bristows.com

Bristows LLP is a limited liability partnership governed by English Law (Registered Number OC358808) and is authorized and regulated by the Solicitors Regulation Authority (SRA Number 591711).

bristows.com

26