|  |
| --- |
|  |
| INDUSTRY BEST PRACTICE GUIDE: |
| SCHEDULE 2, PART 1 PARAGRAPH 2 OF THE DATA PROTECTION ACT 2018 |
|  |
| **Version: 8.0**  **Created by**  **CII New Generation Group – Claims Faculty 2013**  **Published by**  **Insurance Fraud Bureau**  [**www.insurancefraudbureau.org**](http://www.insurancefraudbureau.org) |
| **In association with**  **The Chartered Insurance Institute**  [**www.cii.co.uk**](http://www.cii.co.uk) |
| **25 May 2018** |

**Version Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Created by** | **Date** | **Comments** |
| 1.0 | CII New Generation Group | 2nd June 2014 | Version to Weightmans for sign off |
| 2.0 | CII New Generation Group | 25th June 2014 | Weightmans amended document |
| 3.0 | CII New Generation Group | 23rd Feb 2015 | Amended & final review |
| 4.0 | Insurance Fraud Bureau | 24th Feb 2015 | Final review |
| 5.0 | Insurance Fraud Bureau | 23rd April 2015 | Launch version |
| 6.0 | Insurance Fraud Bureau | 29th June 2015 | Amended to remove timescale requirement |
| 7.0 | Insurance Fraud Bureau | 15th July 2015 | Correction to IFIG definition and section 1.1.4 |
| 8.0 | Insurance Fraud Bureau | 25 May 2018 | Amended to new Data Protection Act 2018 references |

Contents

[Definitions 3](#_Toc390881440)

[Introduction 4](#_Toc390881441)

[1.1. Purpose of Document 4](#_Toc390881442)

[1.2. The Aims of the Industry Best Practice Guidance 4](#_Toc390881443)

[1.3. Data Protection and the Crime and Taxation Exemption 4](#_Toc390881444)

[1.4. Background 5](#_Toc390881445)

[1.5. Ownership of Industry Best Practice Guidance 6](#_Toc390881446)

[2. Spirit of the Best Practice Guidance and S.P.A.R.C Methodology 7](#_Toc390881447)

[3. Best Practice 8](#_Toc390881448)

[3.1. Compliance With the Best Practice Guidance Within Your Organisation 8](#_Toc390881449)

[3.2. Suggested Roles and Responsibilities 8](#_Toc390881450)

[3.3. Use of Pre-Defined Templates (Forms RAD1 & RAD2) 8](#_Toc390881451)

[3.4. Branding the Templates 8](#_Toc390881452)

[3.5. Making a Request 8](#_Toc390881453)

[3.6. SPOC Register 9](#_Toc390881454)

[3.7. Responding to Requests 9](#_Toc390881455)

[3.8. Timescales 9](#_Toc390881456)

[3.9. Employee Profiles and Training 9](#_Toc390881457)

[3.10. Escalation of Issues 10](#_Toc390881458)

[3.11. Recording Requests 10](#_Toc390881459)

[3.12. Analysis of Data 10](#_Toc390881460)

[3.13. Supplier Relationships 10](#_Toc390881461)

[4. Collecting Management Information Guidance 11](#_Toc390881462)

[Appendix 1 - RAD1 Form 13](#_Toc390881463)

[Completing RAD 1 Guidance 13](#_Toc390881464)

[FAQ: 14](#_Toc390881465)

[Appendix 2 – RAD2 Form 16](#_Toc390881466)

[Completing RAD 2 Guidance 16](#_Toc390881467)

[FAQ 16](#_Toc390881468)

# Definitions

|  |  |
| --- | --- |
| **CII** | Chartered Insurance Insitute |
| **IFIG** | Insurance Fraud Investigators Group |
| **IFB** | Insurance Fraud Bureau |
| **SPOC** | Single Point of Contact |
| **RAD1** | Request for Access to Data form 1 – used to request data from another organisation |
| **RAD2** | Request for Access to Data form 2 – used to respond to a request for data from another organisation |
| **GDPR** | General Data Protection Regulations [Regulation (EU) 2016/679)] |
| **DPA** | Data Protection Act 2018 |
| **ICO** | Information Commisioner’s Office |

# Introduction

### Purpose of Document

* + 1. This document sets out industry Best Practice Guidance for making and responding to requests made under Schedule 2, Part 1 Paragraph 2 (hereafter Sch2, Part 1, Para 2) of the Data Protection Act 2018. It sets out Best Practice Guidance for subscribing organisations to follow.
    2. This Best Practice Guidance was developed by the CII New Generation Group 2013 through a consultation process focused on the insurance industry.
    3. Although it is initially envisaged that insurers and solicitors will be the main adopters of this Best Practice Guidance, there are no restrictions upon which organisations may adopt this Best Practice Guidance.
    4. This Best Practice Guidance can be used in respect of any request made under Sch2, Part 1, Para 2, e.g. requests for disclosure under the crime exemption made in respect of claims, underwriting or financial crime.

### The Aims of the Industry Best Practice Guidance

* + 1. The aims of this industry Best Practice Guidance are:
* to provide clarity on the use and application of Sch2, Part 1 Para 2 of the DPA within the Insurance industry;
* to improve the quality of requests made under Sch2, Part 1 Para 2 within the insurance industry;
* to improve the quality of responses to requests made under Sch2, Part 1 Para 2 within the insurance industry, even where the data controller is unable or unwilling to disclose the information requested;
* to increase regulatory compliance with the DPA within the insurance industry;
* to significantly reduce the number of requests made under Sch2, Part 1 Para 2 within the insurance industry that do not contain sufficient information for a data controller to make a judgement on whether or not the information requested should be disclosed;
* to increase the number of responses issued to Sch2, Part 1 Para 2 requests within the insurance industry;
* to increase the speed at which requests under Sch2, Part 1 Para 2 of the DPA are responded to within the insurance industry;
* where appropriate, to increase the sharing between insurers of relevant personal data using Sch2, Part 1 Para 2 requests; and
* to establish a controlled agreement with the SPOCs of all participating organisations taking mutual responsibility to keep updated in respect of this Best Practice Guidance.

### Data Protection and the Crime and Taxation Exemption

* + 1. The DPA governs how organisations can use personal information that they hold.
    2. The DPA generally does not permit any person or organisation to disclose personal data regarding a data subject to a third party if it was not made absolutely clear when the relevant personal data were originally collected that such data would be disclosed to that person or organisation, unless the data subject has been informed of, and consented to, that further disclosure.
    3. However, there are certain exemptions to this rule, including the exemption set out in Sch2, Part 1 Para 2.
    4. Sch2, Part 1 Para 2 of the DPA includes an exemption to the non-disclosure provisions within the GDPR. The following Articles of the GDPR do not apply when processing data for the prevention and detection of crime:
  + Article 13(1) to (3) (personal data collected from data subject: information to be provided);
  + Article 14(1) to (4) (personal data collected other than from data subject: information to be provided);
  + Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);
  + Article 16 (right to rectification);
  + Article 17(1) and (2) (right to erasure);
  + Article 18(1) (restriction of processing);
  + Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);
  + Article 20(1) and (2) (right to data portability);
  + Article 21(1) (objections to processing);
  + Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in sub-paragraphs (i) to (ix); and Articles the first data protection principle, except to the extent to which it requires compliance with the conditions in Schedules 2 and 3 to the DPA;
  + the following provisions of the GDPR (the application of which may be adapted by virtue of Article 6(3) of the GDPR)—
    - Article 5(1)(a) (lawful, fair and transparent processing), other than the lawfulness requirements set out in Article 6;
    - Article 5(1)(b) (purpose limitation).

Sch2, Part 1 Para 2 allows an organisation to disclose personal data to a third party in circumstances where that organisation would otherwise be prevented from doing so by the GDPR, where the disclosure and processing of personal data is for one of the following purposes:

* the prevention or detection of crime;
* the apprehension or prosecution of offenders; or
* the assessment or collection of any tax or duty or of any imposition of a similar nature, (the “**Purposes**”); AND

where the application of the non-disclosure provisions in relation to the disclosure in question would be likely to prejudice any of the three Purposes mentioned above.

### Background

* + 1. The CII New Generation Group 2013 chose to create, through industry consultation, this Best Practice Guidance to improve the quality of data sharing under Sch2, Part 1 Para 2 of the DPA within the insurance industry.
    2. Potential issues with the use of the old Section 29(3) exemption from the DPA 1998 that were identified by the 2013 CII New Generation Group included:
* high volume and poor quality Section 29(3) data requests;
* lack of industry consistency for presenting requests made under Section 29(3);
* confusion over what constitutes a valid request under Section 29(3);
* lack of centralised management information within organisations in respect of Section 29(3) requests;
* poor response rates to requests for information made under Section 29(3); and
* data requests under Section 29(3) being ignored altogether.
  + 1. The ICO is the UK`s independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
    2. All adopters of this Best Practice Guidance should familiarise themselves with its general rules and conduct themselves in line with its principles and also with ICO guidance, the GDPR and the DPA.
    3. The ICO has provided a guide explaining the principles of the GDPR and the DPA which can be found on the website [www.ico.org.uk](http://www.ico.org.uk).
    4. The ICO also provides details on exemptions, including Sch2, Part 1 Para 2 of the DPA, which can be found on the website [www.ico.org.uk](http://www.ico.org.uk).
    5. All adopters of this Best Practice Guidance should ensure that they are familiar with these documents and that such documents are made readily available to their staff.
    6. If any organisation which has adopted this Best Practice Guidance is unsure as to the legal position regarding any request made or proposed to be made under Sch2, Part 1 Para 2 of the DPA, or in respect of any response given or proposed to be given to such a request, then that organisation should seek its own legal advice to ensure compliance with the DPA.

### Ownership of Industry Best Practice Guidance

* + 1. Control and management of this industry Best Practice Guidance will be undertaken by the IFB. Key responsibilities of the IFB include:
* acting as an ambassador for the promotion of this Best Practice Guidance;
* managing the list of organisations that have adopted this Best Practice Guidance;
* ensuring that this Best Practice Guidance is kept up to date;
* encouraging additional organisations to adopt this Best Practice Guidance;
* leadership and hosting of a quarterly forum with the support of adopters of this Best Practice Guidance representing their organisations to discuss and try to resolve any issues in respect of the Best Practice Guidance, (the “**IFB Quarterly Forums**”); and
* the control and circulation of the SPOC register comprising details of all adopters of this Best Practice Guidance.
  + 1. The IFB will not act as an arbitrator in the case of any disputes between adopters of the Best Practice Guidance, nor will they deal with complaints by any of the adopters of this Best Practice Guidance.
    2. Adopters are encouraged to resolve any disputes they may have regarding this Best Practice Guidance between themselves.

# Spirit of the Best Practice Guidance and S.P.A.R.C Methodology

* 1. By adopting this Best Practice Guidance, organisations agree to:
* comply with the GDPR and the DPA;
* abide by the spirit of this Best Practice Guidance, including by:
  + ensuring that their employees make requests under Sch2, Part 1 Para 2 of the DPA only where it is necessary and appropriate to do so;
  + ensuring that due consideration is given to Sch2, Part 1 Para 2 requests received by them as data controllers;
  + ensuring that when personal data are requested under a Sch2, Part 1 Para 2 request, but they cannot or are unwilling, as data controllers, to disclose such personal data to the requester, a detailed reason is provided to the requester;
  + ensuring that their staff are appropriately trained in the use of Sch2, Part 1 Para 2 , both in circumstances where organisations are acting as data controllers and where organisations are acting as data requesters;
  + ensuring that their SPOC details are kept fully up to date with the IFB; and
  + ensuring that a representative attends and fully participates in the IFB Quarterly Forums which are organised the IFB.

**The S.P.A.R.C Methodology**

**When making a request under Sch2, Part 1 Para 2 of the DPA, put yourself in the position of the reviewer/recipient of the request and consider whether you would be satisfied with the level/content of information provided to justify the request. A good test for this is ‘S.P.A.R.C’ methodology.**

The S.P.A.R.C. Methodology should be used to assist those making a request and/or responding to a request under Sch2, Part 1 Para 2 of the DPA to ascertain whether that request is compliant, by considering:

The **S**ubjectmatterof the data request and whether this has been clearly set out in the request.

The **P**roportionality of the information requested in relation to the investigation requirements of the requester.

Whether there has been a clear **A**rticulation of concerns by the requester and how the requested data are relevant to one or more of the Purposes, (i.e. the commission or threatened commission of a particular crime, the apprehension or prosecution of particular offenders and/or the assessment or collection of any particular tax, duty or imposition of a similar nature).

Consideration should be given to whether the data requested are **R**elevant to the crime or taxation Purposes being investigated.

The requestor should be able to clearly state what **C**rime or taxation Purpose they are investigating.

# Best Practice

### Compliance with the Best Practice Guidance within Your Organisation

* + 1. Compliance with this Best Practice Guidance should be the responsibility of the Claims Director, Underwriting Director, Data Protection Officer or another suitably senior nominated person.

### Suggested Roles and Responsibilities

* + 1. Claims Director, Underwriting Director, Data Protection Officer or another suitably senior nominated person - responsible for ensuring that the relevant organisation complies with the terms and conditions of this Best Practice Guidance.
    2. Fraud Manager - responsible for day to day compliance with this Best Practice Guidance for the relevant organisation and the IFB’s principle point of contact in respect of this Best Practice Guidance.
    3. SPOC - responsible for co-ordinating the receipt of responses for the organisation and for being the other adopters’ principle point of contact in respect of day to day queries.
    4. Fraud/Intelligence Handlers - responsible for the day to day despatch and response to requests in strict compliance with this Best Practice Guidance.
    5. Case Handlers - responsible for the identification of requests and compliance with this Best Practice Guidance.

### Use of Pre-Defined Templates (Forms RAD1 & RAD2)

* + 1. When making a Sch2, Part 1 Para 2 request the Form RAD1 template should be used – see Appendix 1.
    2. When responding to a Sch2, Part 1 Para 2 request the Form RAD2 template should be used – see Appendix 2.
    3. Each request and response must be completed on their own merits. It is not acceptable to pre-fill the templates – doing so goes against the spirit of this Best Practice Guidance.
    4. Guidance on how to complete the Form RAD 1 and Form RAD2 templates is set out in Appendices 1 and 2 to this Best Practice Guidance.

### Changing the Templates

* + 1. No changes to the Form RAD1 and Form RAD2 templates should be made, without the agreement of the IFB.

### Making a Request

* + 1. As noted above, when making a Sch2, Part 1 Para 2 request Form RAD1 must be completed – see Appendix 1.
    2. Any request mustcomply with the data protection provisions of the GDPR and DPA.
    3. When making a Sch2, Part 1 Para 2 request, the requester should be satisfied that the content of the request is sufficient to satisfy the relevant data controller that it can disclose the information requested under Sch2, Part 1 Para 2.
    4. A requester should use the S.P.A.R.C. Methodology to assist in this process – see Section 2.
    5. Requesters should refer to the IFB maintained SPOC register to establish which email address the request should be sent to.
    6. Requesters should attach completed Form RAD1s to an email containing a digital ‘signature’ confirming who is making the request. This should contain the name, title and contact details of the individual making the request on behalf of the relevant organisation and the name of the relevant organisation.
    7. Requesters should ensure that the request is sent in line with the relevant organisation’s policy on the safe transfer of data e.g. encrypted email.
    8. Where a response to a Sch2, Part 1 Para 2 request has not been received within a reasonable time, it is recommended that paper chasers are kept to a minimum and only used where the requested information is still required.

### SPOC Register

* + 1. Each adopter must submit details of a SPOC for DPA requests to the IFB for publication on its central register.
    2. The name, role and contact details of the SPOC must be provided.
    3. Each organisation should provide details to the IFB of a centralised email account from which Sch2, Part 1 Para 2 requests made by that organisation and to which responses in respect of any such requests made to that organisation should be sent.
    4. Each organisation must keep its entry in the SPOC register up-to-date, informing the IFB of any change prior to the change taking place.
    5. The IFB will regularly circulate the up-to-date SPOC register to all adopters of this Best Practice Guidance.

### Responding to Requests

* + 1. When responding to a request Form RAD2 must be completed – see Appendix 2.
    2. Any response mustcomply with the data protection provisions of the GDPR and DPA.
    3. Whenever an organisation receives a Sch2, Part 1 Para 2 request, such organisation should refer to the IFB SPOC Register to validate the requestor’s contact details. If there is any uncertainty then contact must be made with the SPOC.

### Timescales

* + 1. All Sch2, Part 1 Para 2 requests which are received by an organisation should be responded to as quickly as possible to maximise potential benefits.

### Employee Profiles and Training

* + 1. In respect of each adopter of this Best Practice Guidance, it is suggested that only the Claims Director, Underwriting Director, Data Protection Officer or other suitable senior person nominated by each adopter of this Best Practice Guidance, the Fraud Manager, the SPOC and the Fraud/Intelligence Handlers should be responsible for making and responding to requests.
    2. Those responsible for making and responding to requests should have undergone appropriate training in respect of Sch2, Part 1 Para 2.
    3. Where a Case Handler has not undergone training and wishes to make or respond to a request, then the request or response Form RAD1 or Form RAD2 templates, as the case may be, should be thoroughly reviewed and countersigned by a person within the relevant organisation who has received appropriate training.
    4. It is recommended that all Case Handlers within each organisation that has adopted this Best Practice Guidance receive internal DPA awareness training to ensure that they can identify a Sch2, Part 1 Para 2 request.

### Escalation of Issues

* + 1. Repeated non-compliance with this Best Practice Guidance by an adopter of this Best Practice Guidance or systemic issues within a relevant organisation should be discussed at the IFB Quarterly Forums or alternatively by utilising existing relationships between adopters of the of this Best Practice Guidance.
    2. As noted above, the IFB will promote use of this Best Practice Guidance and facilitate the IFB Quarterly Forums, but will not in any way act as an arbitrator in the case of any disputes between adopters of this Best Practice Guidance nor will they deal with complaints by any adopters of this Best Practice. Adopters are encouraged to resolve any disputes they may have regarding the Best Practice between themselves.

### Recording Requests

* + 1. All incoming and outgoing requests made under Sch2, Part 1 Para 2 of the DPA should be recorded centrally within your organisation. Guidance on recording requests is set out in section 4.1 of this Best Practice Guidance.
    2. It is suggested that adopter of this Best Practice Guidance builds on the minimum information to conduct a more detailed analysis as set out in Section 4 of this Best Practice Guidance below.

### Analysis of Data

* + 1. The data collected under Paragraph 3.11 of this Best Practice Guidance should be analysed by each organisation on a regular basis. Any trends and/or training needs should be identified and a root cause analysis in respect of such trends and/or training needs completed to determine appropriate corrective action.
    2. Each adopter of this Best Practice Guidance should review such data to ensure it’s compliance with this Best Practice Guidance. It is suggested that this should involve a review of the volume of compliant Sch2, Part 1 Para 2 requests incoming and outgoing and the speed of responses.
    3. Any training needs in respect of Sch2, Part 1 Para 2 requests which are identified should be resolved as soon as possible.
    4. It is suggested that benefits of compliance with this Best Practice Guidance are tracked and recorded, with output shared at the IFB Quarterly Forums, as appropriate.

### Supplier Relationships

* + 1. It is recommended that adherence to this Best Practice Guidance should form part of each adopter organisation’s technical audit and supplier audit process.
    2. This Best Practice Guidance is not intended to override any pre-existing or internal service or contractual agreements between insurers and their service providers.
    3. It is expected that when sharing information, suppliers used by insurance companies will comply with Sch2, Part 1 Para 2 of the DPA and adhere to the processes set out in this Best Practice Guidance.

# Collecting Management Information Guidance

* 1. The following provides a basic framework for the collection of management information, (“**MI**”) relevant to this Best Practice Guidance:
* Making a request under Sch2, Part 1 Para 2 of the DPA:
  + name of the organisation the request has been sent to
  + reason for request (which of the Purposes does the requester wish to process the relevant personal data for, i.e. the purposes of the prevention or detection of crime, the apprehension or prosecution of offenders, and/or the assessment or collection of any tax or duty or any imposition of a similar nature?)
  + details of the nature and extent of the personal data requested
  + details of the specific Purposes the requested personal data will be used for
  + details of why the requested personal data cannot be obtained from another source
  + details of why not releasing the requested personal data would be likely to prejudice/significantly harm the stated Purposes
  + reference number (requester’s organisation)
  + reference number (responder’s organisation)
  + date request was sent
  + date request was responded to if a response is received
  + details of how the request was responded to (Options: Fully; In Part; No Response-No Information; No Response-Not Compliant; No Response-Not Specific)
  + did the response help achieve a saving?

Responding to a request under Sch2, Part 1 Para 2 of the DPA:

* + name of the organisation who has made the request
  + reason for the request (which of the Purposes does the requester wish to process the relevant personal data for, i.e. the purposes of the prevention or detection of crime, the apprehension or prosecution of offenders, and/or the assessment or collection of any tax or duty or any imposition of a similar nature?)
  + details of the nature and extent of the personal data provided
  + details of the specific Purposes the personal data provided will be used for
  + details of why the requested personal data cannot be obtained from another source
  + details of why not releasing the requested personal data would be likely to prejudice/significantly harm the stated Purposes
  + reference number (requester’s organisation)
  + reference number (responder’s organisation)
  + date request was sent
  + date request was responded to
  + details of how the request was responded to, (Options: Fully; In Part; No Response-No Information; No Response-Not Compliant; No Response-Not Specific)
  + did the response help achieve a saving?

Below is an example MI template:



# Appendix 1 - RAD1 Form

****

This document is to be used when making a request under Sch2, Part 1 Para 2 of the DPA, (see Section 3.5)

## Completing RAD 1 Guidance



(To open, right click on the document and choose ‘Presentation Object’ and ‘Edit’).

This document is to be used as guidance on how to complete Form RAD1.

The purpose of this document is to clarify what information is required, why that information is required and why the form is formatted in the way it is.

All fields are mandatory (unless stated otherwise) to ensure compliance with the DPA and this Best Practice Guidance. Failure to complete Form RAD1 correctly may result in information not being shared.

## FAQ:

**Q: Why is Form RAD1 in Microsoft Word (and not Excel, which allows more data to be added)?**

A: It was decided to produce Form RAD1 in Microsoft Word (as opposed to Excel) to allow ease of inputting data - the request needs to contain sufficient information for the responding organisation to be able and willing to share the requested information. Free text is encouraged, as the view following consultation was that template content has no place in fraud enquiries.

**Q: What if my request relates to multiple data subjects?**

A: If a request relates to multiple data subjects, please complete a new Form RAD1 in respect of each data subject.

**Q: Can I edit the form in any way?**

A: The template Form RAD1 should not be edited in any way other than to input the relevant information. If the template Form RAD1 is edited, it will lead to non-standard Sch2, Part 1 Para 2 requests being made which are likely to be rejected by the responding organisation that is being asked to provide the requested information.

**Q: What if I think the form should be changed - what is the process for doing that?**

A: Suggested alterations to the template Form RAD1 should be raised with the IFB at the IFB Quarterly Forums. The IFB is authorised to agree any changes to the template Form RAD1 and issue updated versions to all adopters of this Best Practice Guidance.

**Q: Why aren’t there drop down lists (e.g. for suspected crime etc.)?**

A: Use of drop down lists was considered for certain areas of Form RAD1, however through consultation it was agreed that drop down lists could lead to requesters not properly considering every aspect of the request, leading to more non-compliant requests.

**Q: How do I send a RAD1 Form?**

A: Completed Form RAD1s should be sent in PDF format, attached by email. Requesting organisations should follow their own internal IT security policies, but it is recommended that all emails containing Form RAD1 requests should be encrypted where possible.

**Q: Which pieces of information are mandatory?**

A: Completion of all parts of Form RAD1 is mandatory, apart from the ‘either/or’ boxes highlighted in this Best Practice Guidance (e.g. the date of birth or National Insurance number of the relevant data subject, or additional information if none is available). This is to ensure that the responding organisation has all the information it requires to be able to respond to a request where possible. Failure to complete all areas of Form RAD1 will increase the risk of a request not being met.

**Q: How do I know who to send requests to?**

A: Form RAD1s should be sent by the requester to the relevant contact at the organisation that the Sch2, Part 1 Para 2 is being sent to as included in the IFIG maintained DPA request contact list. In the absence of a published contact, the requestor must consider the most appropriate contact at the organisation that the Form RAD1 is being sent to.

# Appendix 2 –RAD2 Form

****

This document is to be used when responding to a request made under Sch2, Part 1 Para 2 of the DPA, (see Section 3.7)

## Completing RAD 2 Guidance



(To open, right click on the document and choose ‘Presentation Object’ and ‘Edit’)

This document is to be used as guidance on how to complete Form RAD2.

The purpose of this document is to clarify what information is required, why that information is required and why the form is formatted in the way it is.

## FAQ

**Q: Do I need to respond to every request made under Sch2, Part 1 Para 2 of the DPA?**

A: To maximise the benefits of this Best Practice Guidance, every adopter of this Best Practice Guidance should try and respond to all requests made under Sch2, Part 1 Para 2 of the DPA (even if non-compliant), even if it is to confirm that the requested personal data will not be provided to the requester. This will ensure that there is confidence that all Sch2, Part 1 Para 2 requests are being reviewed and any non-compliance issues can be addressed to help increase compliance across the insurance industry. The number of non-compliant Sch2, Part 1 Para 2 requests should therefore reduce over time.

**Q: What do I need to consider when deciding if a Sch2, Part 1 Para 2 request is compliant?**

A: The responding organisation must carefully consider any request set out in a completed Form RAD1 and satisfy itself that such request complies with Sch2, Part 1 Para 2 of the DPA.

The responder must complete in full the version controlled Form RAD2 in respect of all requests for personal data made under Sch2, Part 1 Para 2 of the DPA and return the completed Form RAD2 to the relevant requester.

There is a duty placed on responding organisations to ensure that any personal data that they release in response to a request for personal data made under Sch2, Part 1 Para 2 is appropriate and relevant in the context of the request made, (please see below for further details of the ‘S.P.A.R.C.’ Methodology, which is intended to assist a responding organisation in this regard).

Responding organisations should remember that data controllers are not legally compelled to share information under Sch2, Part 1 Para 2 of the DPA, if they choose not to do so (unless the requester obtains a court order requiring the release of the requested personal information).

**S.P.A.R.C.:**

**S = Subject of Data**

* It is important that a responding organisation understands who the main data subject/s are in respect of each request that it receives under Sch2, Part 1 Para 2 of the DPA. The data subject is the individual about whom the requester wishes to obtain data.
* Generally speaking, the data subject dictates the context by which it can be decided whether any requested information is relevant and proportionate to the processing of the requested personal data for the stated Purpose(s).
* If, for example, medical report data is requested pertaining to a stated data subject’s injuries and that data subject is suspected of fraud, the request is likely to be relevant as it relates to an individual who has been identified as a suspected fraudster.

**P = Proportionality**

* Even if a crime is suspected, this will not justify the sharing of every piece of potentially relevant information without thought.
* Responding organisations should take care not to provide requesters with more information than has been requested.
* The specific information requested should be considered carefully, taking into account all known suspicions, in deciding whether providing the requested data is proportionate to the investigation’s requirements of the requester.

**A = Articulation of Concerns**

* The responding organisation must be satisfied that reasonable concerns/reasons exist which directly relate to the suspected crime (or other Purpose) stated by the requester and which would justify disclosure of the relevant personal data under Sch2, Part 1 Para 2 by the responding organisation taking into account:
  + the reason for the request (which of the Purposes does the requester wish to process the relevant personal data for?)
  + the nature and extent of the personal data requested
  + the specific Purposes the personal data provided will be used for
  + why the requested personal data cannot be obtained from another source
  + why not releasing the requested personal data would be likely to prejudice/significantly harm the stated Purposes
* The responding organisation does not need full sight of every last piece of evidence or intelligence held by the requester which would justify releasing relevant personal data, but it should have sight of the key evidence or fraud indicators which justify the release of the requested data under Sch2, Part 1 Para 2 of the DPA.
* In cases of suspected fraud, the test should be that, when presented with the facts, would the responding organisation have concerns that fraud is taking place?

**R = Relevance**

* The responding organisation must be satisfied that all requested data is relevant to the particular crime being investigated, or other stated Purpose.
* The responding organisation should consider this by asking itself what information it would request when investigating the same matter.
* The responding organisation should only consider disclosing the requested personal data if it can clearly be put to use by the requestor in investigating or defending a fraud or other crime, (or in the pursuit of another stated Purpose).

**C = Crime**

* The responding organisation must be satisfied that a criminal act (or some other Purpose) is being investigated. The responding organisation must be clear as to exactly what is being alleged.
* In the context of the insurance industry the crime that requesters will be trying to prevent will usually be fraud and may include: fraud by false representation; fraud by failing to disclose; and/or fraud by abuse of position.
* Many requests made under Sch2, Part 1 Para 2 of the DPA in the context of the insurance industry are likely to relate to organised fraud, motor fraud and opportunistic motor/casualty insurance frauds.

**Q: In what format should I make the response?**

A: Completed Form RAD2s should be sent in PDF format, attached by email. Responding organisations should follow their own internal IT security policies, but it is recommended that all emails containing Form RAD2 responses should be encrypted where possible.