Standard Operating Procedure

Title:	**Data Subject Rights Standard Operating Procedure**		
Version:	**1.0**	**Effective Date**	**October 2018**
Summary:	Describes the various procedures for servicing data subject rights under the GDPR and Data Protection Act 2018		

When using this document please ensure that the version you are using is the most up to date by checking on the University's online document system http://documents.manchester.ac.uk/list.aspx for any new versions.

1 Background and purpose

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 confer several rights on individuals about whom the University holds and processes personal data. The University must administer requests from individuals relating to these rights in order to remain compliant with the legislation.

This standard operating procedure is designed to set out the processes involved when the University receives a request from a data subject in relation to any of the data subject rights provided by the GDPR or Data Protection Act 2018.

Adherence to this procedure ensures that the University adheres to established procedures when servicing data subject rights requests, in order to:

- ensure that the University's responses to such requests are consistent across the institution;
- ensure that the University's responses to such requests are undertaken in a timely and efficient manner;
- minimise the risk of data subject complaints to the Data Protection Regulator;
- minimise the risk of the University committing a technical breach of data protection legislation, and the reputational and financial consequences thereof;
- ensure that personal data is held in a fair, legal and transparent manner;
- ensure that all areas of the University are familiar with their responsibilities in the event of a data subject request.

2 Definitions and scope

2.1 Definitions

- **Data Subject** refers to any identifiable living individual about whom the University processes personal data.
- **Data Controller** refers to the body, in this case the University, which alone or jointly with others determines the purposes and means of the processing of personal data. Most of the data which the University holds about individuals is processed on a controller- subject relationship, so subject rights apply.
- **Personal Data** means any information relating to an identified or identifiable natural person, whether held in a structured or unstructured form.
- **Data Processing** means any operation performed on personal data by automated or manual means, including collection, recording, organisation, structuring, storage, adaptation or

alteration, retrieval, consultation, use, disclosure, alignment or combination, restriction, erasure or destruction.

- **Data Subject Rights** refers to the several rights conferred by the GDPR on individuals exercisable against data controllers. These rights are available to anybody about whom the University holds personal data as a data controller (including children aged 13 and above) subject to certain exemptions.

2.2 Scope

This procedure applies to all processing of personal data by the University and all aspects of servicing the rights of data subjects. This could potentially involve any member of staff at the University (particularly for subject access requests), but will particularly impact on the Information Governance Office, IT Services, Human Resources (HR) and the Directorate for Student Experience (DSE).

2.3 Research data

Data held solely for research purposes is exempt from most of the data subject rights detailed below provided that:

- the application of the rights would prevent or seriously impair the achievement of the objectives of the research in question;
- no decisions are being taken about individual participants as a result of the research project; and
- the research has in place appropriate safeguards to protect the rights and privacy of individuals whose data is being processed.

The latter will be ensured through the appropriate Ethics Committee, and research which involves the processing of personal data must obtain ethical approval.

In some circumstances the right to object to processing could apply to data held for research purposes. Staff must contact the Information Governance Office (" IGO") if they receive such a request relating to a research project.

In the interests of fairness and transparency it may be that the University will in any case wish to respond positively to rights requests from participants, particularly if to do so will not adversely affect the conduct or outcome of the relevant project. Many of these requests will be dealt with as business as usual by researchers. For example, if a participant wishes to be removed from a project and their data erased then this can be dealt with locally.

The IGO will need to be involved in some circumstances however, in addition to the objections to processing mentioned above. Subject access requests received for research data, whether or not the data will be supplied, must be administered through the IGO. Also, any rights request which is to be refused will need to be administered by the IGO as appropriate grounds for refusal will need to be supplied to ensure compliance with the legislation.

3 <u>Procedure and responsibilities</u>

The University has separate procedures for each of the data subject rights. The rights are as follows: access to data, data portability, rectification of data, erasure of data, restriction of processing, objection to processing and prevention of automated decision making.

When a data subject rights request is received by the University it is the responsibility of the IGO to validate the request and provide an initial response. As many data subject rights requests are subject to statutory time limits it is important that these reach the IGO as soon as possible after receipt. All University staff therefore have a responsibility to be able to recognise the types of request outlined in this SOP and to forward them to the IGO if they are received locally.

The IGO is responsible for ensuring requests are forwarded to the relevant area in a timely manner and engaging with them to ensure that any queries about the requests are dealt with. In the case of subject access and portability requests the IGO is also responsible for assessing the information, determining the applicability of exemptions and where necessary preparing it for disclosure. The Head of Information Governance is ultimately accountable for the responsibilities of the IGO.

The procedure for the receipt and validation of subject rights requests can be found in Appendix A.

3.1 The right of access

The right of access to information (data subject access right) obliges controllers to provide individuals with access to their data and with information about how their data is processed. The controller must confirm whether personal data is being processed about the data subject and provide a copy of that data (subject to exemptions and the rights and freedoms of third parties). The University must also inform the data subject of the purposes of the processing, the categories of data involved, recipients of the data, the retention period for the data, the source of the data and any automated decision making or international transfers involving the data.

Subject access requests (SARs) under this right are the most common data subject rights requests received by the University. Due to the nature of the University's extensive data infrastructure and the University's sometimes complex relationship with its data subjects, subject access requests are also often very resource intensive. A data subject can request any and all information held about them by the University, and therefore a SAR can potentially involve any member of staff who has had recorded contact with the data subject. SARs often involve data from personal email boxes and P Drives for example.

The University has one calendar month to supply the data and associated information, and can only extend this under exceptional circumstances.

All members of University staff must be aware of the right of access to personal data and must manage their data accordingly. It is possible that any staff member will be asked to provide data about individuals with whom they have had professional contact, including students and fellow members of staff, so information recorded about this contact must be appropriate, retrievable and managed in accordance with the University retention schedule. Requested data must be provided to the IGO as soon as possible and certainly within the time limit defined by the IGO when the request is assigned. The deadline for the provision of information provided by the IGO is set following consideration of the volume of work required to both locate the information and for the IGO to assess it, apply exemptions and prepare the information for disclosure (e.g. applying redaction, removing duplicates) and meet the statutory deadline.

Some subject access requests, such as those for CCTV footage and for information from the Division of Development and Alumni Relations ("DDAR") follow particular and separate procedures.

The detailed procedure for responding to a subject access request can be found as Appendix B to this SOP. CCTV and DDAR exceptions can be found as Appendix C and Appendix D.

The procedure for data subjects who wish to appeal against the outcome of SARs is detailed in Appendix E.

3.2 The Right to Erasure

Under Article 17 of the GDPR data subjects have the right to request that personal data about them processed by the University be erased under certain circumstances. Data need only be erased if its continued processing would be inconsistent with the requirements of the GDPR or otherwise unlawful. The data subject does not need to prove harm or distress to exercise this right.

The circumstances under which data must be erased upon request include the following:

- data are no longer necessary in relation to the purpose for which they were collected;
- processing was undertaken on the basis of the data subject's consent, but that consent has been withdrawn;
- there is no overriding legitimate legal basis for continued processing of the data; or
- data is processed for direct marketing purposes, and the data subject wishes this data to be erased.

In a similar manner to the subject access procedure, the bulk of responsibility for servicing right to erasure requests will fall upon the IGO and IT Services. Also similar to the SAR procedure is the fact that data about an individual may be held by any member of staff, and the IGO may need to undertake a search to identify data to be erased.

Members of University staff must respond in a timely manner to requests from the IGO for information held about individuals who have requested erasure, and certainly within the timescale requested by the IGO when the request is made.

In addition, to reduce the burden of requests under the right to erasure University staff must ensure that personal data is retained only for as long as is allowed by the University Retention Schedule.

Where processing is undertaken on the basis of consent, these consents must be properly recorded, a mechanism for withdrawal of consent must be provided to the data subject, and data for which consent is withdrawn must be destroyed promptly.

The process for administering erasure requests is detailed in Appendix F.

Erasure requests for data held by DDAR are subject to an exception process which is detailed in Appendix G.

3.3 The Right to Data Portability

Article 20 of the GDPR entitles a data subject to receive a copy of data which they have supplied to a data controller on the basis of consent or for a contractual purpose and which the University is processing through automated means. The copy must be in a structured, commonly used and machine readable format so that the data subject can transfer this data easily to another data controller if they so wish.

Data portability requests which concern the provision of staff and student data from core systems will be dealt with as business as usual requests by the HR and the DSE. Other requests will be dealt with by the IGO and IT Services.

The process for administering data portability requests can be found as Appendix H.

3.4 The Right to Rectification

Article 16 of the GDPR entitles data subjects to request that data held about them which is inaccurate or incomplete be rectified.

The data subject is also entitled to be informed if inaccurate or incomplete data has been disclosed to third party recipients, and the University has the duty to inform these third parties of the rectification, unless this would involve disproportionate effort.

The University is entitled to take a view on the accuracy and completeness of data which may vary from that of the data subject, and refuse to rectify data on demand. The data subject would then have a right of appeal to the Information Commissioner's Office (ICO).

Rectification requests will be dealt with by the IGO and IT Services in conjunction with the business area of the University which owns the data in question.

In order that the impact of rectification requests upon the University can be minimised, it is important that all staff ensure that the data which they process relating to data subjects is complete and accurate, and that regular data quality assurance exercises are undertaken for University systems.

The University process relating to data rectification requests can be found at Appendix I.

3.5 The right to object to automated decision making

Article 22 of the GDPR restricts data controllers from making decisions about individuals based solely on automated means, where those decisions will have a significant impact on individuals.

Data subjects who feel that they have been subject to wholly automated decision making have the right to complain to the ICO or to take legal action.

Data controllers can use wholly automated decision making by consent provided that the process is fair and transparent and sufficiently explained to the data subject. Advice on this must be obtained from the IGO if such processing is envisaged.

University members of staff must ensure that the University does not undertake processing which involves decisions being taken about individuals by wholly automated means and without human input. This is particularly true where the processing could have a significant impact on an individual (for example an admissions or recruitment decision) or where special category personal data such as health, sexuality, ethnicity or religious belief are involved.

Any new process which involves automated decision making about individuals must undertake an Information Governance risk review.

It is very unlikely that the University will receive a complaint relating to automated decision making, but if it does the relevant procedure can be found at Appendix J.

3.6 The right to object to processing

Article 21 of the GDPR confers rights on data subjects to object to the processing of data which is being used by the data controller for public interest or research purposes, or for the controller's legitimate interests. Such objections must be related to the individual circumstances of the data subject and the processing, and so each request will need to be dealt with on a case by case basis. The University may continue processing the data if it can prove an overriding justification for doing so.

The IGO will administer objections to processing in conjunction with the relevant business area and, if necessary, IT Services.

The relevant procedure can be found at Appendix K.

3.7 The right to object to direct marketing

Article 21 also confers upon data subjects the right to require controllers to stop using their data for direct marketing purposes. This includes the right to prohibit profiling for marketing purposes and to prevent the sending of marketing messages by means including post, email, text, telephone and online.

The right to object to marketing is absolute and controllers are obliged to cease such activity upon request. The objection applies to all processing of the individual's data for the purposes of direct marketing beyond the actual sending of marketing materials. So if an individual objects to direct marketing any information held by the University solely for marketing purposes must be erased, and data not held solely for such purposes must be flagged as not to be used for marketing.

As marketing is carried out by many different areas of the University it is likely that many objections will be received locally and will be actioned under business as usual processes. Local business areas which carry out direct marketing must ensure that they have local procedures for quickly and comprehensively removing data from marketing processes for individuals who request this.

Institution-level objections will be administered by the IGO, and the relevant process can be found at Appendix L.

3.8 The right to restriction of processing

In certain circumstances data subjects have the right to require a data controller to restrict processing of their personal data. Data for which processing is restricted can be stored but not used in any other way unless the data subject consents.

The circumstances under which such restriction would be appropriate would include if the accuracy of the data were disputed by the data subject, if the data were being processed unlawfully but the data subject preferred restriction to erasure, where the legitimacy of the processing was under dispute between the University and the data subject or where the data subject required the data to be retained for longer than its retention policy for the purposes of a legal dispute.

Where data has been restricted, the University has a duty to inform all third parties to whom the data has been disclosed, so long as the effort involved in doing so is not disproportionate. The data subject has the right to be informed of any such disclosures.

Processing restriction requests will be unusual and specific to particular circumstances, and so will be administered by the IGO in conjunction with local business areas and IT Services. The procedure for dealing with such requests can be found at Appendix M.

4 Monitoring compliance with the Procedure

4.1 Enforcement

Heads of School, Directors or equivalent are accountable for ensuring that all staff within their area act in accordance with this Procedure.

4.2 Audit

Evidence of the effective administration of data subject rights will be audited periodically.

4.3 Reporting

The Head of Information Governance will report on this Procedure to the Information Governance Committee.

5 Review of Procedure

This Procedure will be reviewed at least every two years or when significant changes are required.

6 Contact list for queries related to this procedure

Role	Name	Telephone	Email
Head of Information Governance	Tony Brown	0161 306 2106	Tony.brown@manchester.ac.uk
Head of Data Protection (DPO)	Alex Daybank	0161 306 2473	Alex.daybank@manchester.ac.uk
Deputy Head of Information Governance	Barbara Frost	0161 275 2122	Barbara.frost@manchester.ac.uk

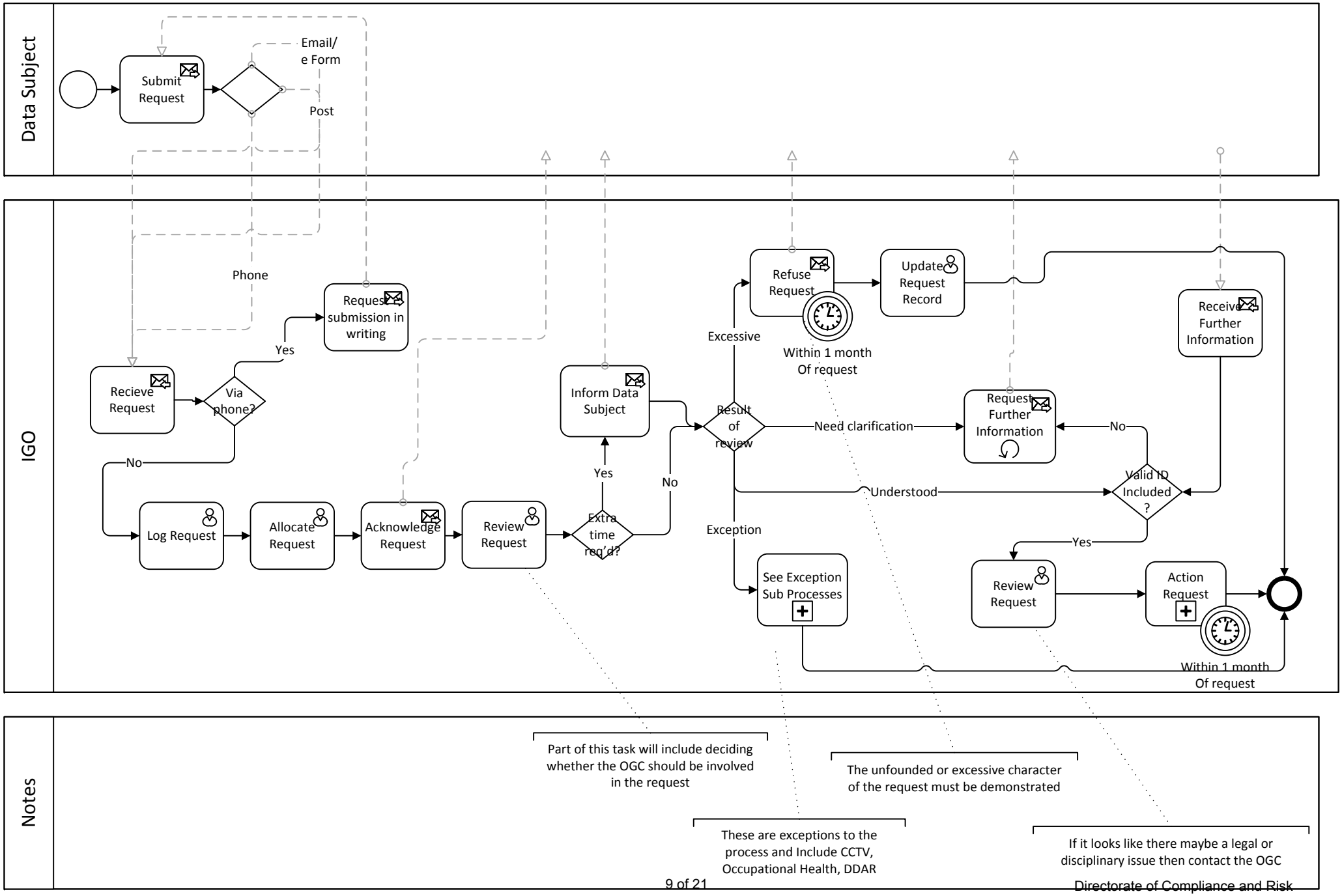
Version control

Version	Date	Reason for change
1.0	September 2018	Creation

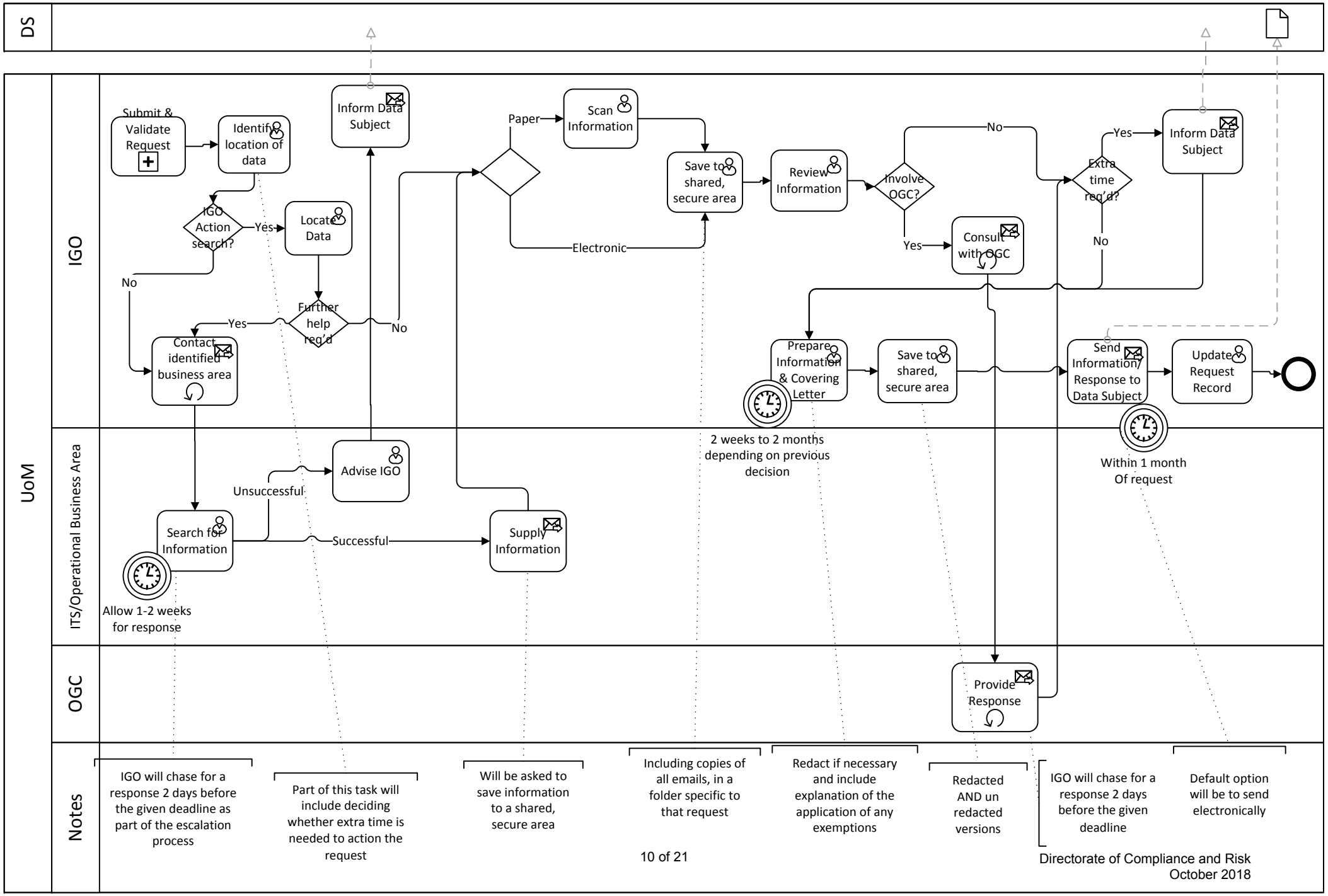
Document control box	
Procedure title:	**Data Subject Rights Standard Operating Procedure**
Date approved:	4 October 2018
Approver:	Information Governance Committee
Version:	1.0
Supersedes:	N/A
Previous review dates:	
Next review date:	September 2020

Related Statutes, Ordinances, General Regulations:	• Ordinance XIV Intellectual Property Rights (IPR), Data Protection and the Use of Information Systems • University General Regulation XV Use of Information System
Related policies:	• Information Security Policy http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=6525 • Data Protection Policy http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=14914
Related procedures:	• Information classification, ownership and secure information handling: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=29971 • Financial Procedures: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=1742 • Contracts Governance Policy: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=7926 • Technical Security Standards: http://www.itservices.manchester.ac.uk/aboutus/policy/
Related information:	• Records retention schedule: http://documents.manchester.ac.uk/display.aspx?DocID=6514
Procedure owner:	Head of Information Governance

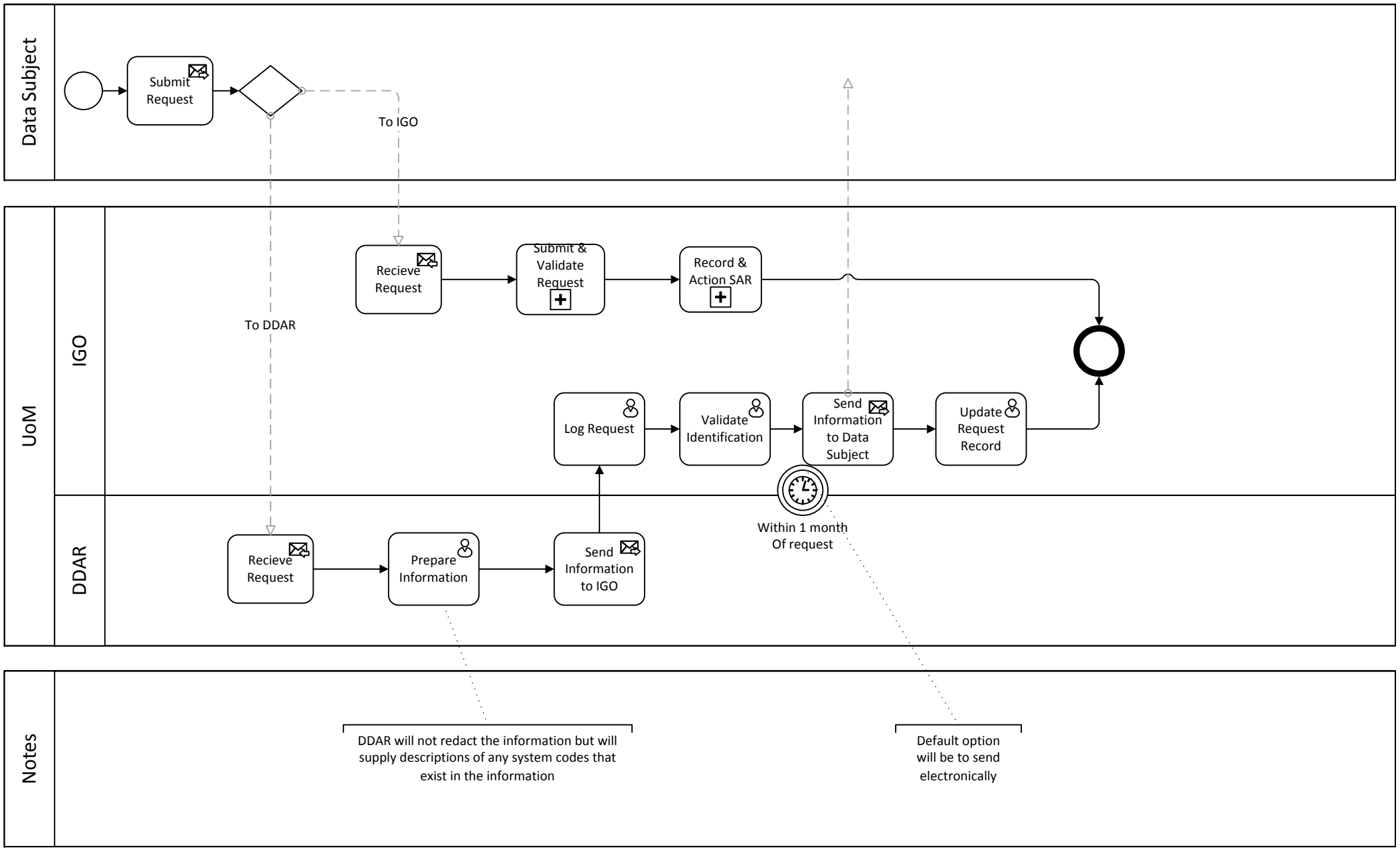
Appendix A Rights Request - Submit & Validate Request



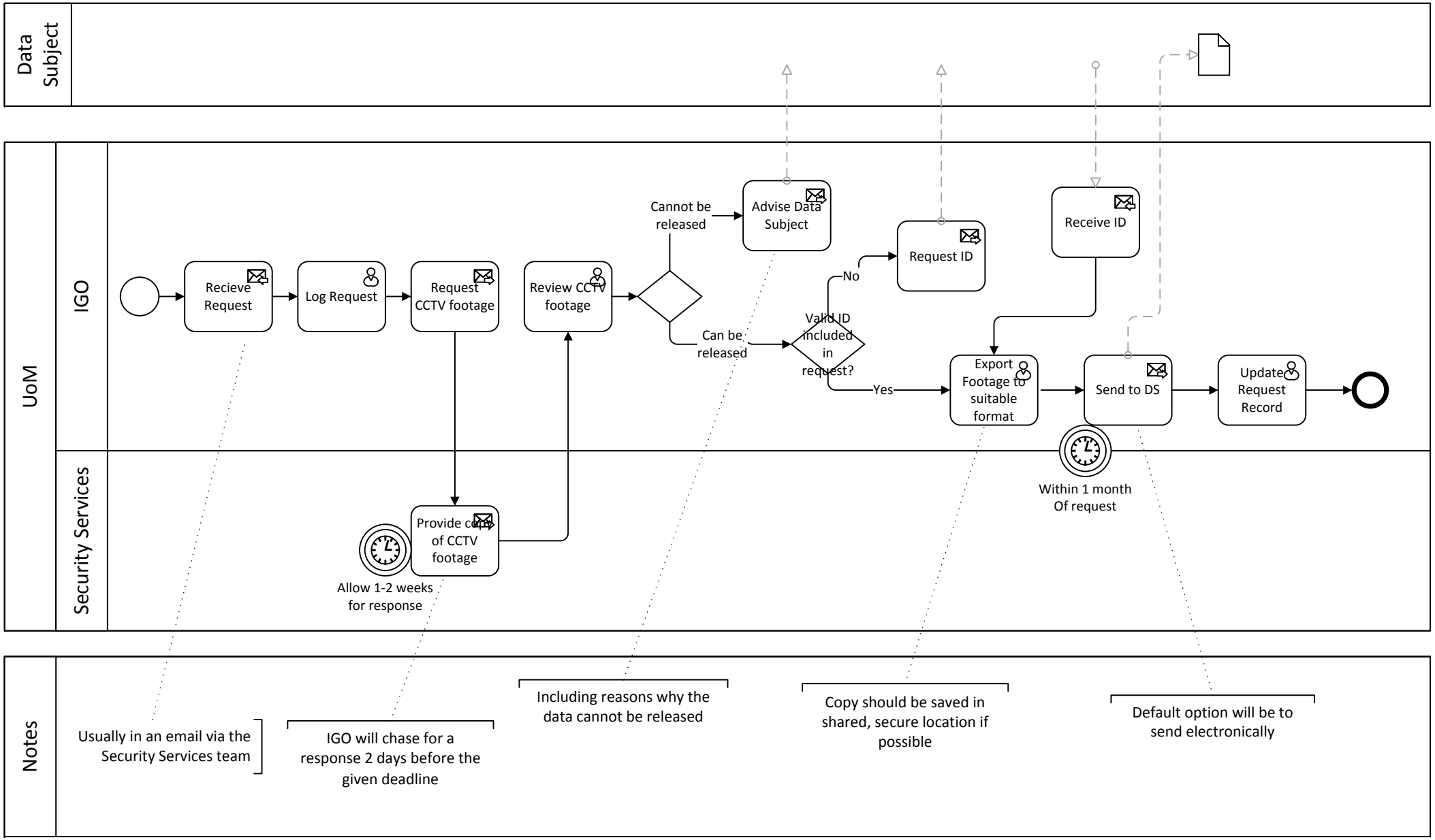
Appendix B Right to Access - Action Request



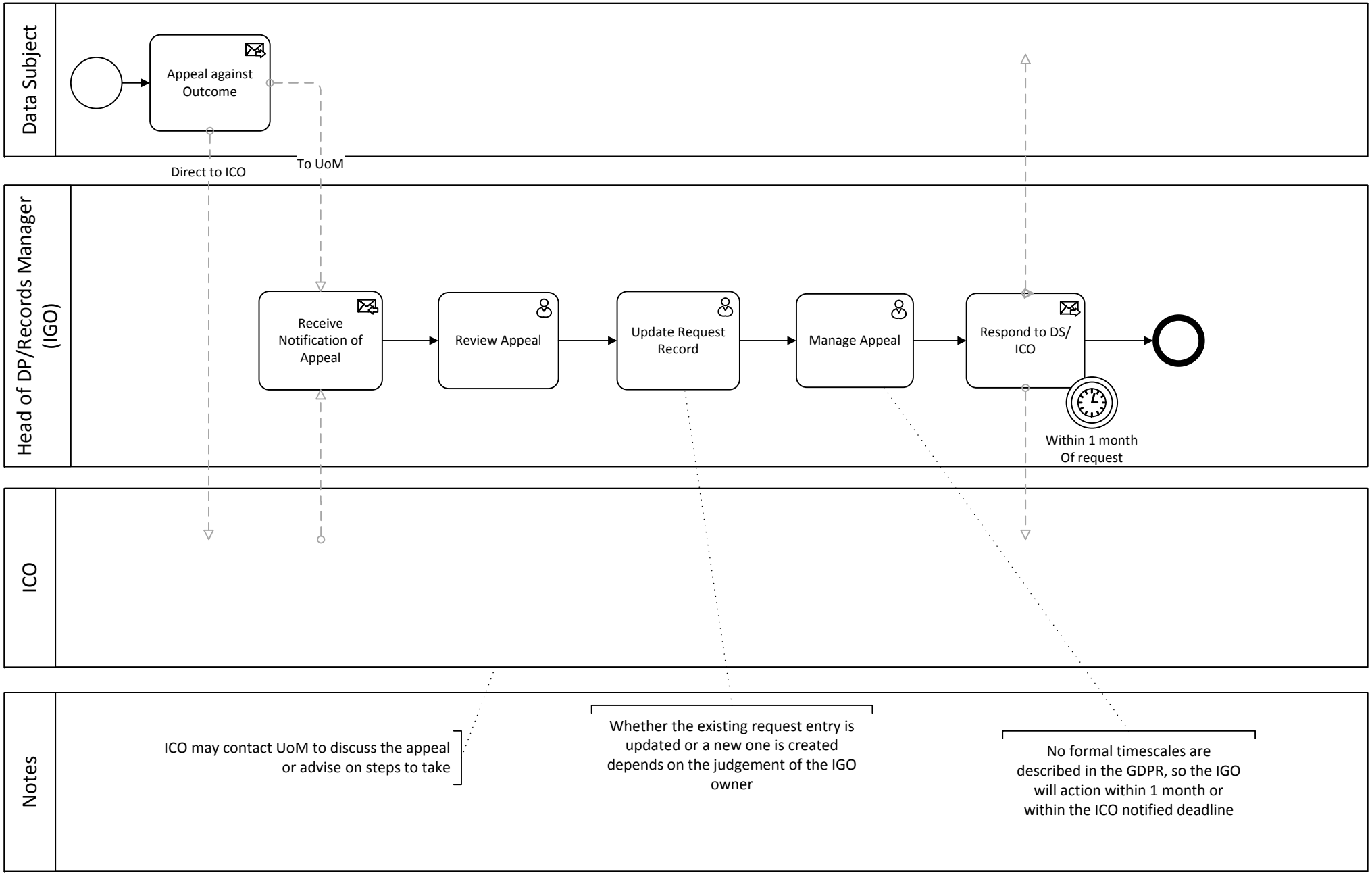
Appendix C Right to Access Exception - DDAR



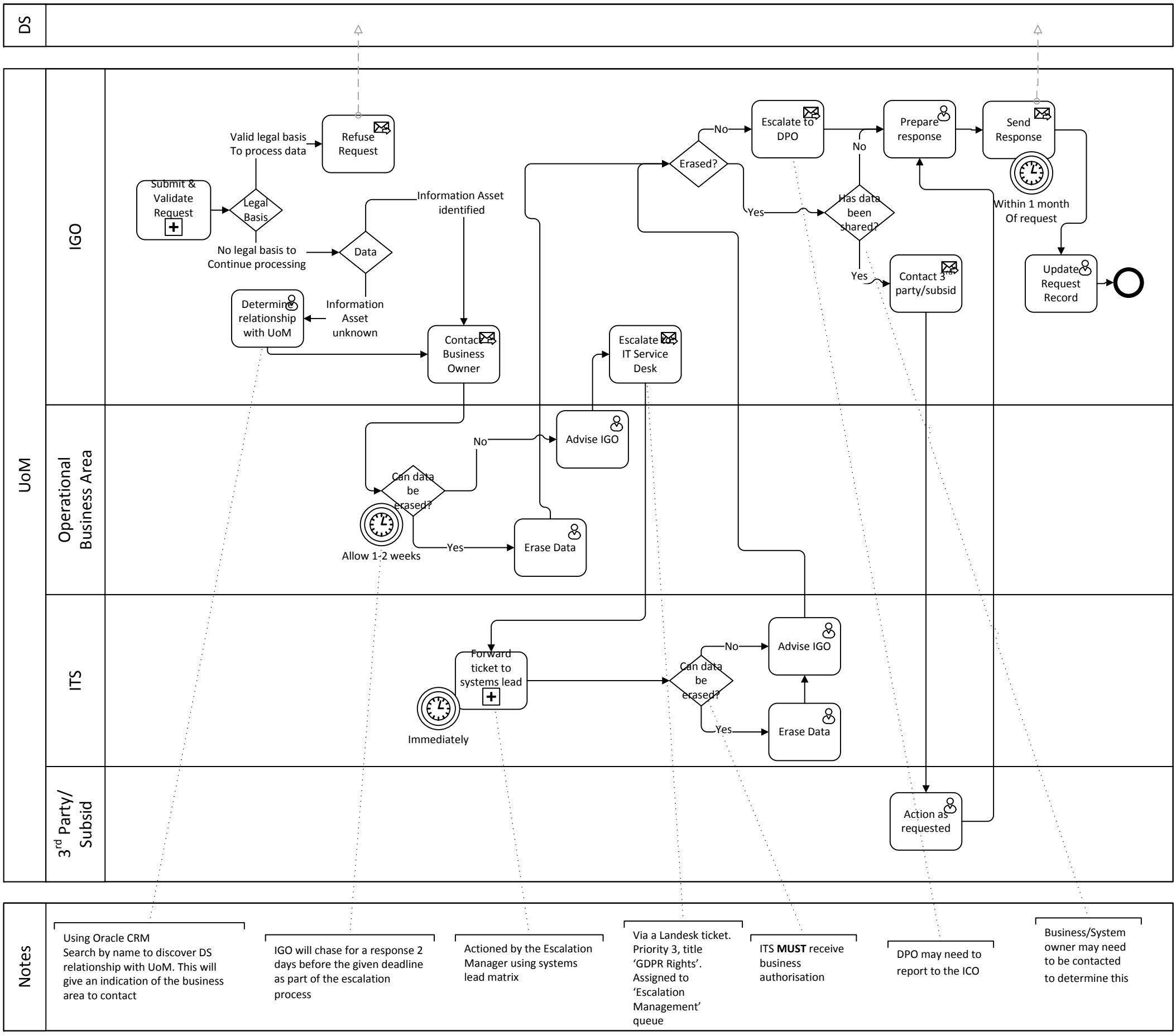
Appendix D Right to Access Exception - CCTV



Appendix E Rights of the Data Subject
- Appeals

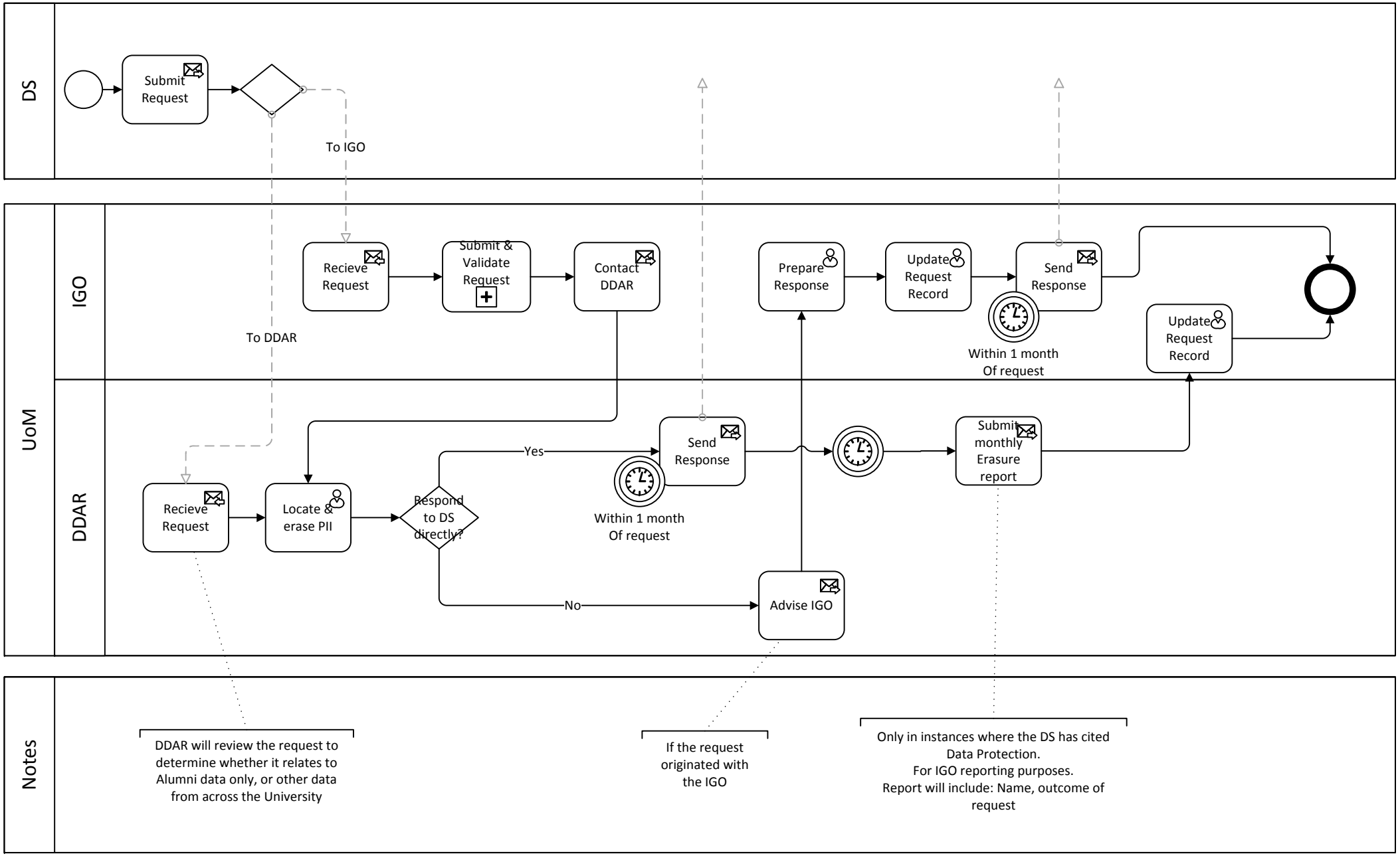


Appendix F Right to Erasure – Action Request

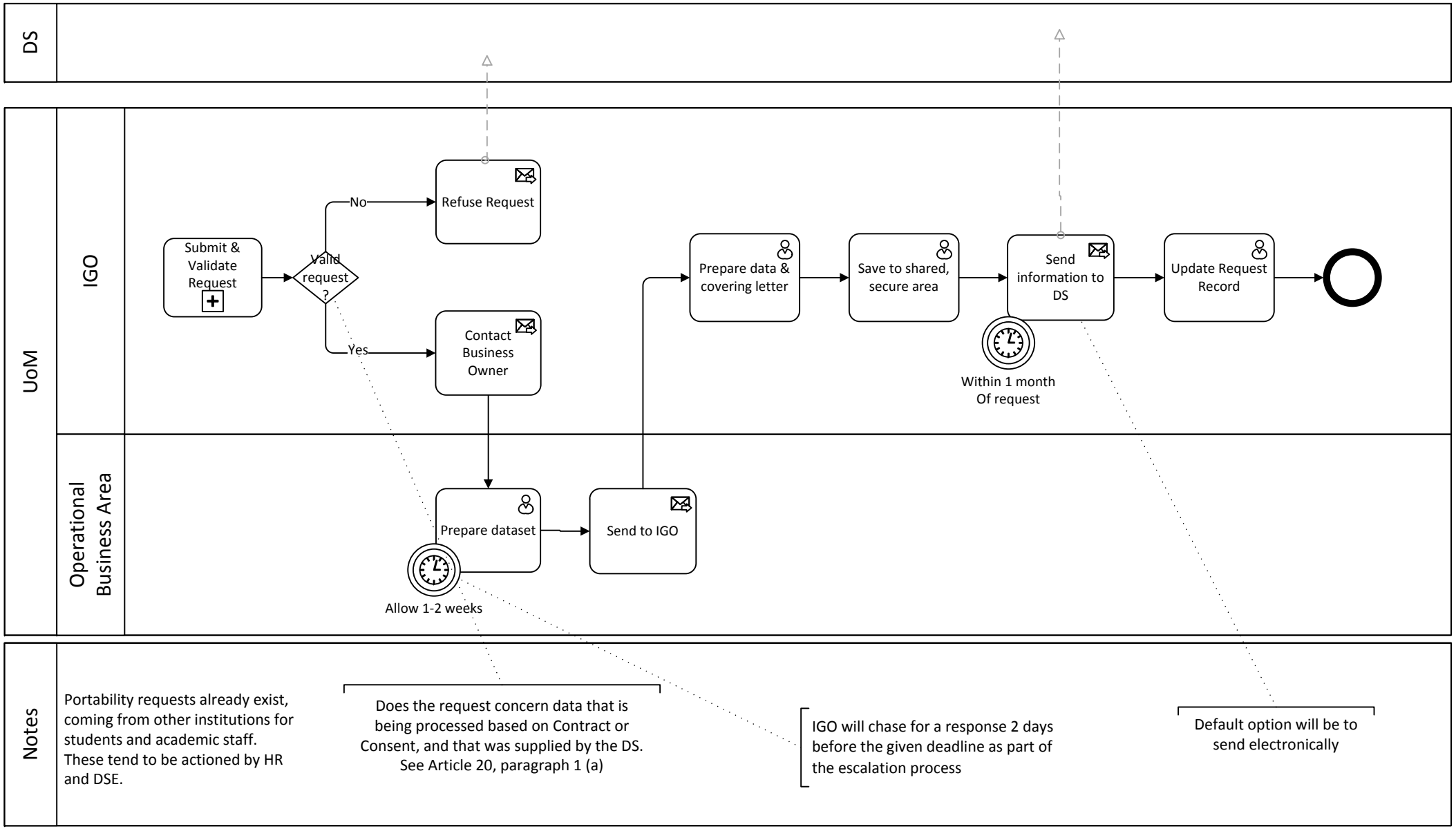


Notes							
Using Oracle CRM Search by name to discover DS relationship with UoM. This will give an indication of the business area to contact	IGO will chase for a response 2 days before the given deadline as part of the escalation process	Actioned by the Escalation Manager using systems lead matrix	Via a Landesk ticket. Priority 3, title 'GDPR Rights'. Assigned to 'Escalation Management' queue	ITS **MUST** receive business authorisation	DPO may need to report to the ICO	Business/System owner may need to be contacted to determine this	

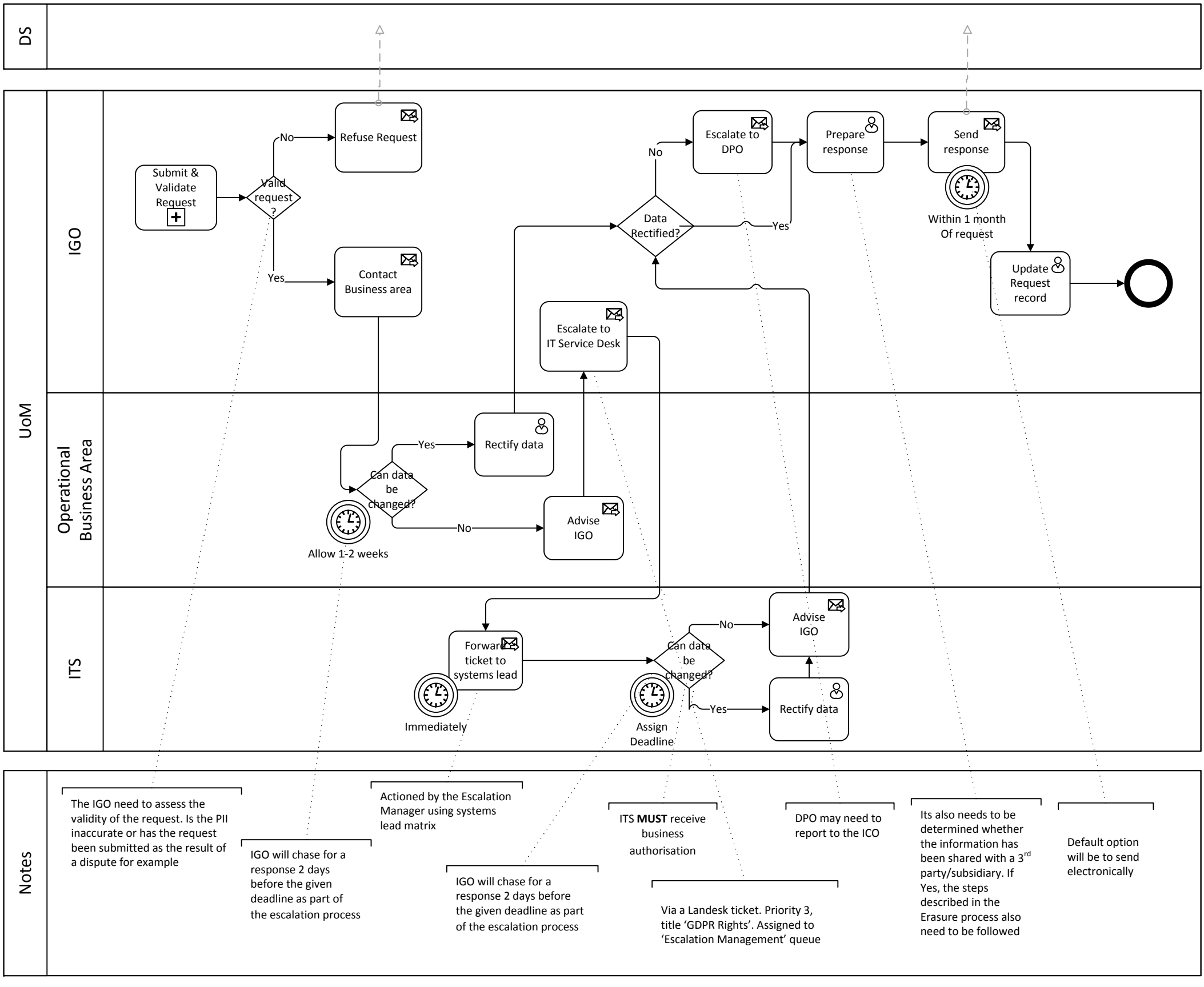
Appendix G Erasure Exception - DDAR



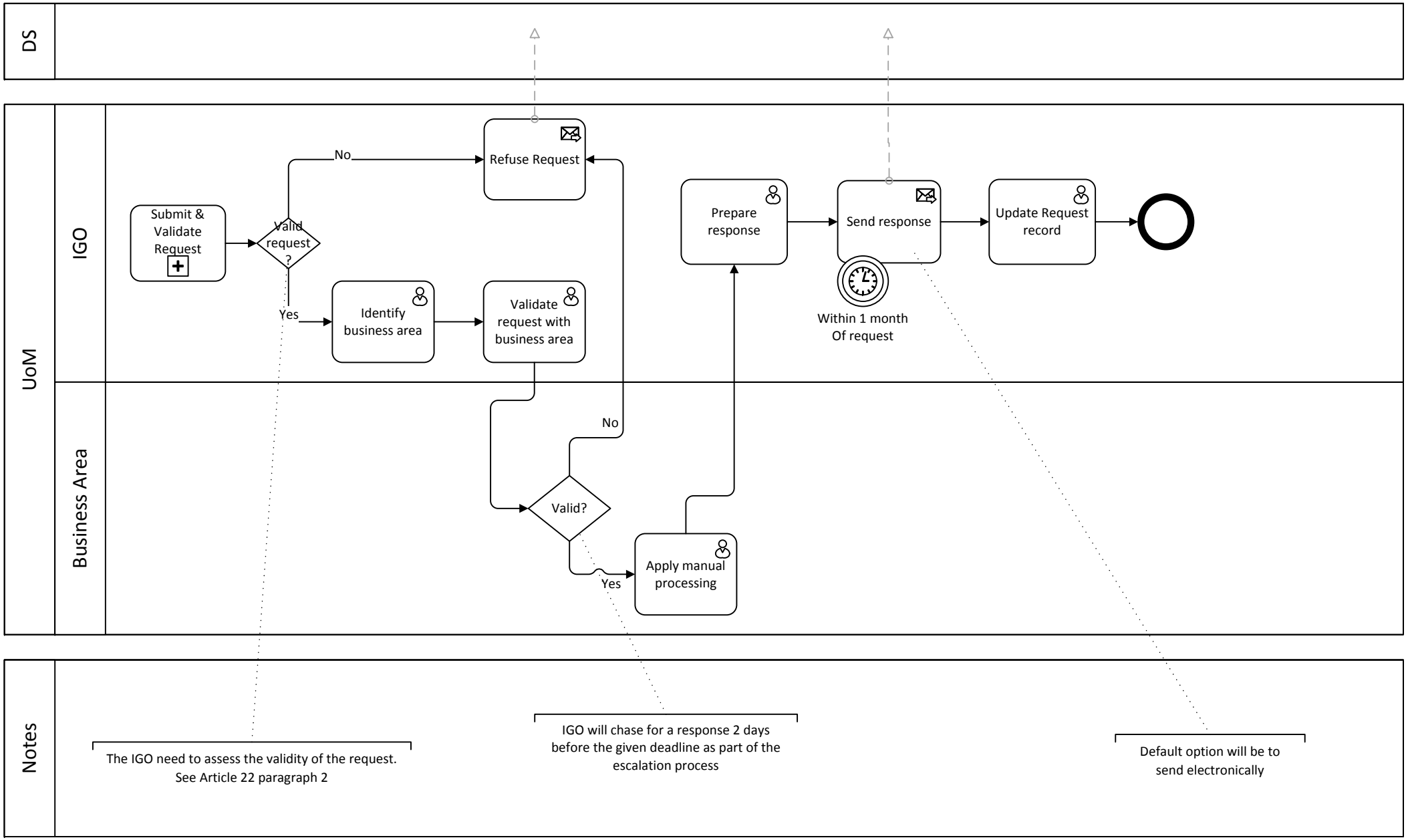
Appendix H Right to Data Portability – Action Request



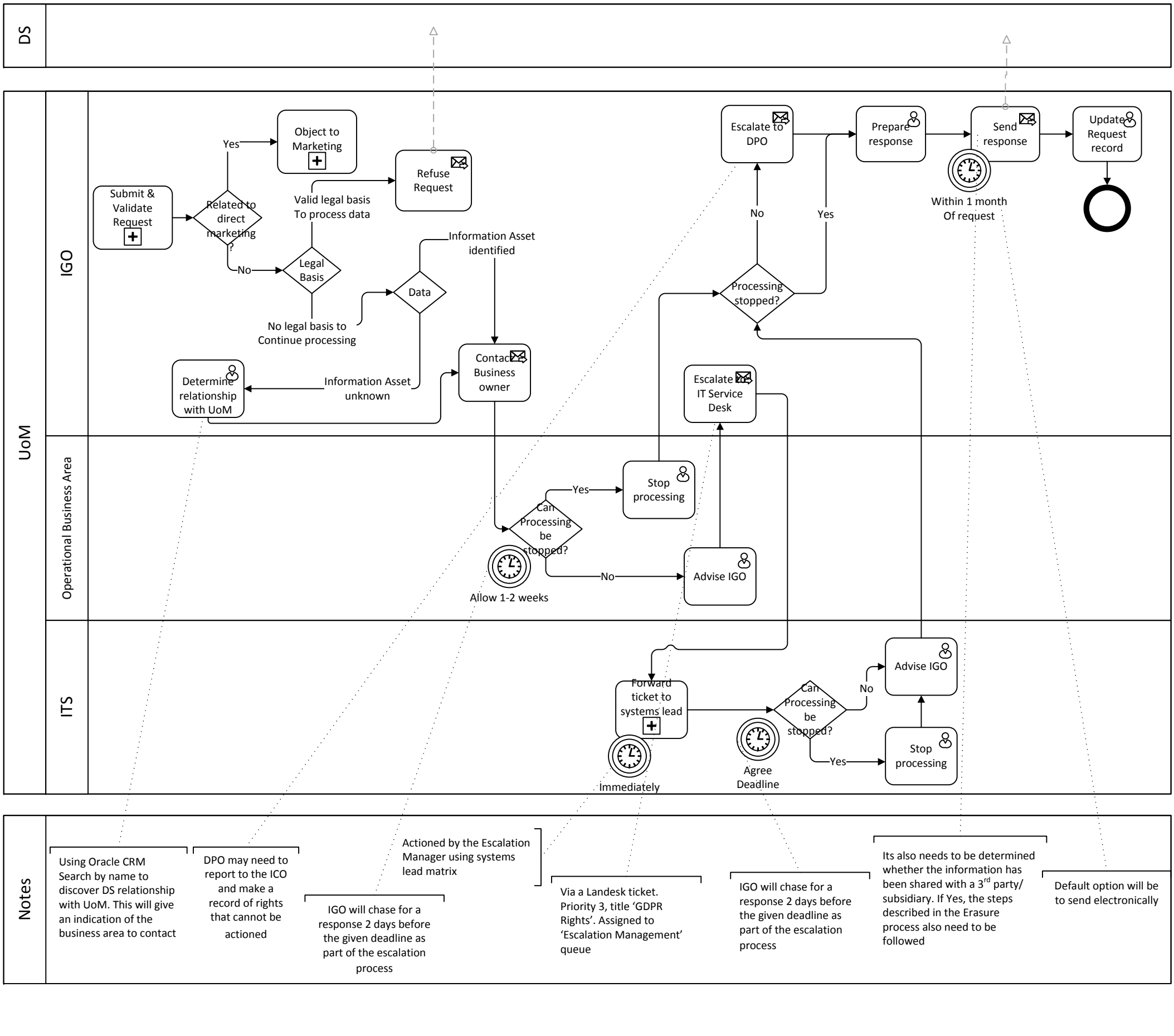
Appendix I Right to Rectification – Action Request



Appendix J Automated Individual Decision Making - Action Request



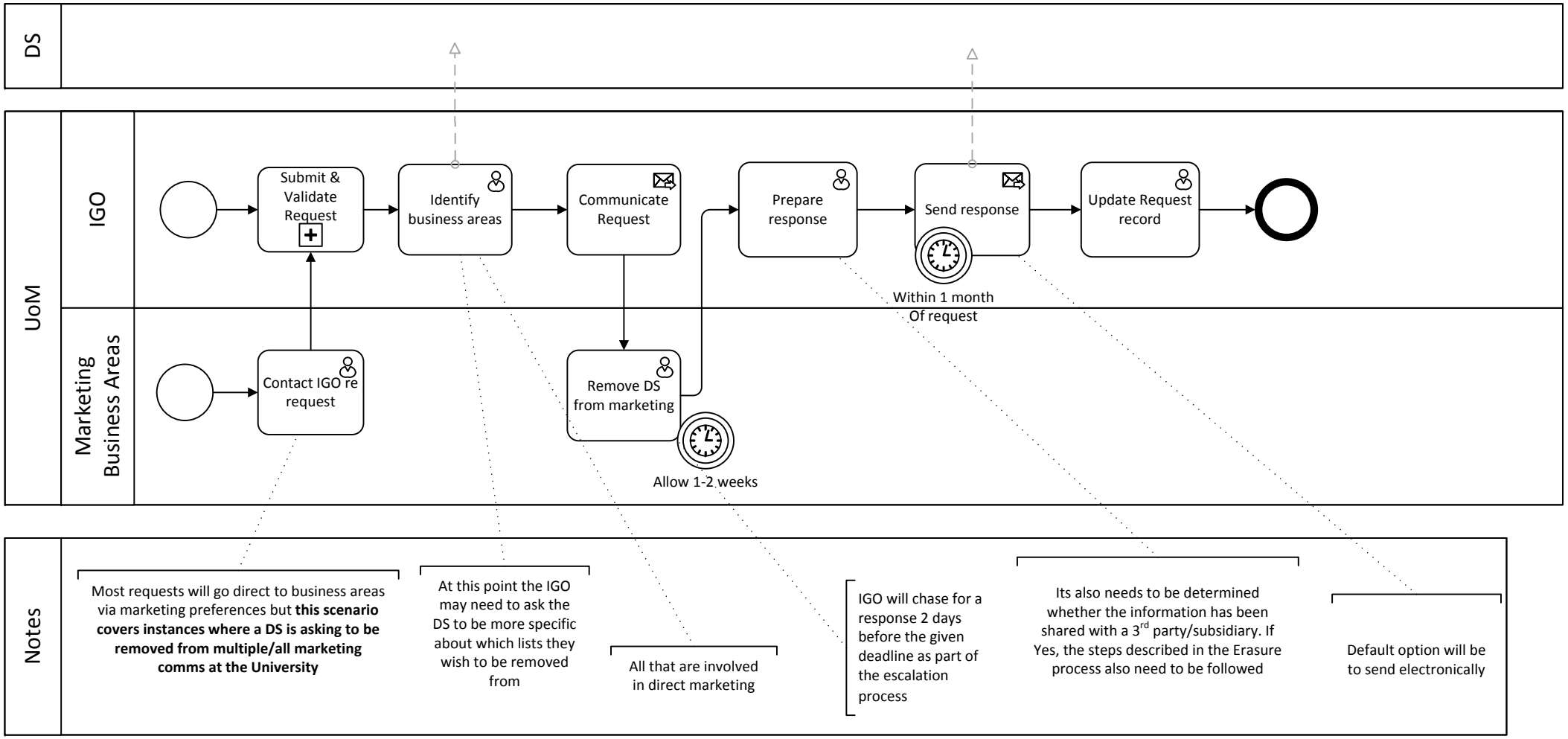
Appendix K Right to Object - Action Request



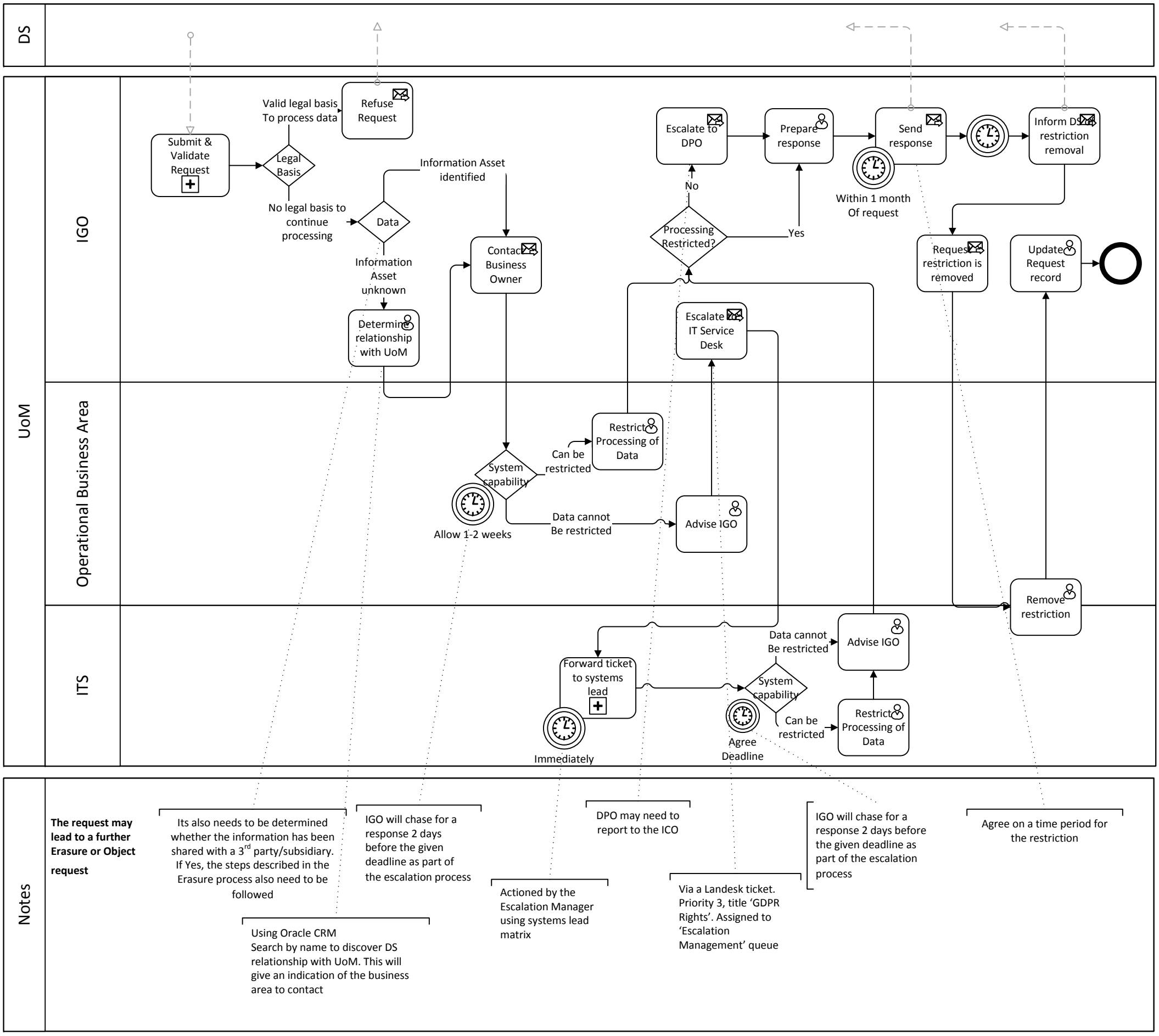
Notes

- Using Oracle CRM Search by name to discover DS relationship with UoM. This will give an indication of the business area to contact
- DPO may need to report to the ICO and make a record of rights that cannot be actioned
- IGO will chase for a response 2 days before the given deadline as part of the escalation process
- Actioned by the Escalation Manager using systems lead matrix
- Via a Landesk ticket. Priority 3, title 'GDPR Rights'. Assigned to 'Escalation Management' queue
- IGO will chase for a response 2 days before the given deadline as part of the escalation process
- Its also needs to be determined whether the information has been shared with a 3rd party/ subsidiary. If Yes, the steps described in the Erasure process also need to be followed
- Default option will be to send electronically

Appendix L Right to Object (Marketing) - Action Request



Appendix M Right to Restriction of Processing



Notes

The request may lead to a further Erasure or Object request

Its also needs to be determined whether the information has been shared with a 3rd party/subsidiary. If Yes, the steps described in the Erasure process also need to be followed

Using Oracle CRM
Search by name to discover DS relationship with UoM. This will give an indication of the business area to contact

IGO will chase for a response 2 days before the given deadline as part of the escalation process

Actioned by the Escalation Manager using systems lead matrix

DPO may need to report to the ICO

Via a Landesk ticket. Priority 3, title 'GDPR Rights'. Assigned to 'Escalation Management' queue

IGO will chase for a response 2 days before the given deadline as part of the escalation process

Agree on a time period for the restriction