Policy and Procedure for approving, monitoring and reviewing personal data processing agreements

POLICY

Authors: Mr Peter Wilson
Approved By: PME
Date: 23 April 2009
Version: 1.0

Personal data processing by external suppliers, contractors, agents and partners

Policy and Procedure for approving, monitoring and reviewing personal data processing agreements

Policy on contracting with external suppliers, contractors, agents and partners to process personal data

1.1. **Personal data** is any information

- That relates to a living person who can be identified by that information, ether by itself or in combination with other data.

The University is legally obliged to process personal data in accordance with the Data Protection Act, 1998, and has a duty of care to all of its data subjects (people whose personal data we hold). Misuse of personal data by employees, including accidental or deliberate loss or disclosure to third parties, puts the University at legal and reputational risk and is likely to result in disciplinary action.

1.2. This policy and procedure must be followed whenever

1. The University intends to contract with an external supplier, contractor, agent or partner (**a contractor**) to provide a service for the University AND
2. the University needs to share personal data it already holds, e.g. staff or student data, with the external body to deliver the service OR
3. the University intends to contract with an external body to collect and process personal data in order to deliver the service for the University

Under these circumstances, the contractor will be acting as a **Data Processor** for the University. **Under the Data Protection Act, 1998, (DPA) the University is legally liable for any breaches of data security by the Data Processor.**

1.3 This policy and procedure must be followed for all procurement involving transfer of personal data or outsourcing of data processing to third parties, in conjunction with and in addition to the University's Standard Conditions of Contract. The procedure must be followed as part of the procurement and selection process so that potential contractors and suppliers are fully aware of our information security requirements and able to demonstrate how they will meet them before a contractual agreement is signed.

1.4 Before agreeing to transfer the data, the person delegated to commission the external service on behalf of the University (The Authorised Contact) will follow the procedure set out in section 2 for seeking approval for the data transfer. This procedure is designed to help users navigate through the stages of the process using a questionnaire format for ease of use. This process involves liaising with the Data Protection Officer and other officers responsible for managing the personal data to:

1. Determine whether the proposed data transfer is fair, lawful and appropriate
2. Identify the risks of transferring the data (and of not sharing it) and take appropriate action to reduce their likelihood or mitigate their impact
3. Ensure that the contractor signs the University Data Processing agreement committing them to process the personal data in accordance with the Data Protection Act.

Once the contract and Data Processor Agreement are in place, it is the University's responsibility to

4. Manage the data transfer securely
5. Inform the data subjects appropriately, where necessary,
6. Make stringent, on going checks, to audit that the contractor is fully compliant with all aspects of the DPA

1.5 The Data Processor Agreement, policy and procedure for its use apply worldwide. All personal data transfers from the UK to countries outside the EU must in addition comply with condition 2 of the Agreement.

1.6 This policy and procedure does not apply where

- A third party requests personal data *for their own purposes* e.g. to sell goods and services to students. Third party requests of this kind will be managed as requests for information under the Freedom of Information (Scotland) Act.

1.7 This policy and procedure has been developed to take account of

- Increasing risk of identity theft, fraud and abuse of personal data
- Technological ease of accidental/deliberate loss/disclosure of personal data
- Regulatory requirements
- Stakeholder and public concern about privacy and information security
- Reputational risks arising from breaches of information security.

The policy and procedure will be reviewed regularly and updated as necessary to take account of legal, process, technological and reputational risks.

1.8 Following approval, the FOI and Data Protection Officer will

- Disseminate the policy, procedure and Data Processor agreement to Heads of Schools, Institutes and Services and liaise with them to identify staff roles where the holders need to be briefed and trained to comply with it.
- Liaise with the relevant responsible officers to arrange training for staff
- Liaise with the responsible officers, identified in section 2, below to identify existing arrangements for transferring personal data and outsourcing of personal data handling and apply the policy and procedure retrospectively to these

POLICY

- Liaise with the Director of Procurement Services to incorporate the procedure and Data Processor Agreement into all procurements involving transfer of personal data or outsourcing of data processing to third parties
- Monitor use and compliance with the procedures, maintain a central record of Data Processor Agreements and put in place procedures to monitor compliance with them

Ann Jones
University Archivist, FOI and Data Protection Officer
13 February 2009

POLICY

2. Procedure for approving, monitoring and reviewing personal data processing agreements

Project/activity			
University contact:			
Phone		Email	

Step 1 Do I need to follow this policy and procedure?

Does the proposed project /activity involve the University contracting with an external supplier, contractor, agent or partner (**a contractor**) to provide a service for the University?	YES	NO

If YES

Does the University needs to share personal data it already holds, e.g. staff or student data, with the external body to deliver the service OR	YES	NO
Does the University intend to contract with an external body to collect and process personal data in order to deliver the service for the University?	YES	NO

If YES

The authorised contract must follow the following procedure to obtain University approval before any contract involving transfer or processing of personal data by third parties can be agreed.

Step 2: Who needs to be involved?

The person delegated to commission the external service on behalf of the University (the authorised contact) must seek approval for the data transfer from the Data

POLICY

Protection Officer (DPO) AND the relevant officers responsible for managing the personal data:

The responsible officers are	**Tick all relevant**
The Data Protection Officer	
The Academic Registrar: for student personal data	
The Director of Recruitment and Admissions: for applicant (student) personal data	
The Director of Human Resources: for staff (and applicant- staff) personal data	
The Director of Procurement Services: for projects involving procurement of suppliers	
The Director of Finance and IS/IT: for staff, student or customer personal data in manual or electronic financial systems e.g. fee payments, payroll, tax, pensions	
The Director, University Information and Computing Services (UICS): for authorising a secure method of transferring personal data held in centrally managed IS/IT systems	
The Relevant Head of School/Institute: for authorising a secure method of transferring personal data held in IS/IT systems where management responsibility is delegated to that School/ Institute	
The Group Risk Manager: for reviewing the operational risk assessment	
The Director of Corporate Communications: for agreeing a communication plan, where necessary, detailing how and when people need to be informed e.g. by all staff or student email.	

For example: an arrangement to transfer staff salary data to an external pensions provider would require the approval of the Data Protection Officer, Directors of Human Resources, Finance and IS/IT and UICS. Once the approved Data Processor Agreement is in place, it is not necessary for each responsible officer to approve the data transfer each time a new member of staff wishes to join the pension scheme. This is because the procedure includes a process for creating or updating a Fair Processing Notice which the new member of staff would receive when they sign up to the pension scheme, explaining what the University will do with their personal data and advising the data subject of their rights under the DPA.

Step 3: When do I need to do this?

For any project or activity involving 3rd party processing of personal data it is essential to consider whether the processing is necessary and assess the potential information security risks at the earliest stage so that the actions necessary to mitigate these risks can be agreed, planned and completed at the appropriate stages in the project.

POLICY

For projects involving the procurement of services: at the point that you ask *potential* contractors to quote for their services
Specific information security controls must be identified as early as possible in any procurement process and incorporated into the specification issued to potential tenderers and suppliers.

For all other potential data transfers: *before* any agreement is signed
Whether or not the project involves payment for goods or services, potential contractors and partners must be asked to demonstrate how they will comply with our information security requirements *before* any contractual agreements are signed.

Step 4: How do I go about getting approval for the data transfer?
Arrange to meet the DPO, and the relevant responsible officers to review the proposed data transfer/outsourcing of data processing. The review will consider whether the processing is fair and lawful and complies with the 8 Data Protection Principles, identify the risks involved and agree action to mitigate these

At the meeting, review and complete the following checklist. You will need to get some information from the proposed contractor to answer some of these questions.

Date of review	
In attendance	

What does the project involve?
Please append the following as relevant

Project Terms of reference	
Draft procurement specification	

Is the processing necessary?
Is there a viable alternative to sharing the data/outsourcing the data processing? E.g. can the University license and host software rather than sharing staff or student personal data with the third party in order to access the service?

YES/NO	If yes, describe the agreed alternative. If no explain why alternatives are not practicable.

POLICY

What personal data really needs to be processed, why and for how long?
Apply the principle of data minimisation – no more, and no longer, than necessary.

What personal data?	
Why?	
For how long?	
What specific legal conditions (in Schedule 2 of the DPA) allow us to process this data?	DPO to complete this
What needs to be done to destroy the data confidentially?	
Who will do this?	
When?	
What assurance do we need to confirm that the data has been destroyed?	

Does the data include sensitive personal data?

What kind of sensitive personal data?	**YES?**	**Why do you need this?**
Racial or ethnic origin		
Religious beliefs		
Political opinions		
Trade union membership		
Physical or mental health		
Sexual life		
Actual or alleged offences committed		
Any legal proceedings, judgements, sentences against them		
If yes, what specific legal conditions (in Schedule 3 of the DPA) allow us to process this data? DPO to complete this		

Is the proposed use of the data compatible with the *original* purpose for which it was obtained?

YES	NO	We don't currently collect this data

POLICY

Do individuals have a reasonable expectation that their data would be used in this way?

What information do you currently give people about how their data will be used? Please provide a copy of this. (It may be a privacy notice or a declaration that people sign when you collect their data)
How and when do you communicate this to them?

Who is responsible for ensuring the data is accurate and kept up to date?

The University	The contractor	The individual (e.g. self service user)
How will this be done and monitored?		

Does the project involve transferring personal data to countries outside the EU?

YES	NO

If YES, transfer contracts must include the standard clauses for data transfers to non-EU countries (7.1.2005) set out in European Commission Decision C (2004)5271. This is necessary to provide an equivalent standard of privacy protection to the DPA for the individuals whose data will be transferred.

Do we need to obtain the consent of the people whose data we want the contractor to process?

This will depend on several factors. These include (but are not confined to)

Is it essential for the University to process the data in order to fulfil its contractual obligations e.g. paying its staff?	YES	NO
Is it not essential but desirable for the University to process the data e.g. provide and monitor take-up of voluntary training?	YES	NO
Does the data include sensitive personal data?	YES	NO

To be completed by DPO

No consent needed: inform data subjects of the data transfer
Inform data subjects in advance of data transfer and give them the opportunity to opt out
Obtain the explicit, informed and freely given consent of the individuals (an opt in) before sharing the data.
Relevant conditions of processing (DPA Schedules)

POLICY

What are the risks of transferring the data (and of not sharing it)?

Risks of transferring the data

Risk	Mitigating Action
Impact on personal privacy	
Method of transfer	
Governance: policies, procedures	
Human Resources security	
Physical Security	
IT Security	
Subcontracted processing	
Business Continuity	
Retention/destruction	
Legal	
Reputational	
Other	

Risks of not sharing the data

Risk	Mitigating Action
Strategic	
Operational	
Legal	
Reputational	
Other	

Do we need to make a privacy impact assessment?	YES	Not sure	NO
Does the risk need to be on an operational/strategic risk register?	YES	Not sure	NO

If YES/Not sure: escalate to Group Risk Manager

What specific information security controls do we require the data processor have in place to manage the data?

"Organisations cannot simply require that a contractor comply with ISO requirements. That is not an effective way of managing real world risk." - Pinsent Masons.

Requirement for Information security plan included in procurement specification?	YES	NO
Information security plan agreed with contractor?	YES	NO
Does the plan include satisfactory arrangements for		
Method of transfer	YES	NO
Governance: policies, procedures		

Human Resources security		
Physical Security		
IT Security		
Managed destruction of data in accordance with retention policy		
Subcontracted processing		
Business continuity (disaster recovery)		
Incident reporting and management		
Audit of compliance		

In what format/s is the data to be transferred?

Format of data: paper	YES	NO
Format of data: electronic	YES	NO
Not applicable: the service provider will collect the data on our behalf	YES	NO

How will the data be transferred?

Have the DPO and the relevant School/Institute IT officer agreed a secure method of transferring the personal data to the service provider?	YES	NO
Please give details of the proposed transfer method/s		

Step 5: Signing the agreement

Once the security plan and the data transfer method have been agreed, ask the Responsible Officers to sign the Data Transfer Approvals section at the end of the Data Processor Agreement.

Then ask the Data Processor (contractor) to sign two copies of the University Data Processing agreement to process the personal data in accordance with the Data Protection Act; including any specific measures set out in the information security plan, and return both copies to the DPO.

The DPO will sign the Data Processing agreement as the University signatory, returning one copy each to the data processor and the authorised contact and retaining the original signed agreement as part of the central audit trail recording the terms of the agreement.

Step 6: When and how do I need to communicate with the people whose data will be processed?

First: agree with the DPO and the Director of Corporate Communications a Fair Processing Notice (sometimes known as a Privacy Statement). This should explain to data subjects:

- Who is responsible for looking after their data
- How and why their data will be processed,
- Who else may have access to their data and why
- Whether they have the right to opt out or in as appropriate
- Who to contact to access the information held about them or find out more about their rights under the DPA

Second: agree the method and timing of communicating this notice
The communication must be badged as a Heriot-Watt communication with a University contact. The wording of the communication must be agreed in advance with the authorised contact, the DP officer and the responsible officer/s.

Third: Ask the contractor designated as the data processor to liaise with UICS to ensure that there is adequate notice of any email communication the data processor intends to make to staff or students. If this communication is to be by email, the data processor will give details of the email address to be used in communications to UICS so that it can be added to the "white list" of approved email addresses so that University email security systems do not automatically block access to the message or flag it up as spam.

Step 7: At what point can I transfer the data to the contractor or ask them to collect it on our behalf?

Only ***after*** the all of the above steps have been completed.

Step 8: What happens next?
The DPO will liaise with the authorised contact and the Data Processor to monitor compliance with the agreement and security controls.

Version 8. Originally drafted by Ann Jones, Derek G Brown, Kathy Patterson, 29/10/2008. Amended by Ann Jones 13.02.2009 to take account of feedback from users of the procedure and advice from the Group Risk Manager; UICS; Dundas and Wilson; the Information Commissioner's Office; ISO/IEC 27001/2:2005 Information Security Management; HM Government/The National Archives: Managing Information Risk; JISC Legal Code of Practice for the Further and Higher Education Sectors on the Data Protection Act 1998, 2008; Pinsent Masons: Transferring data: the information security issues.

POLICY

Personal Data Processing Confidentiality Agreement between Heriot-Watt University and [….]
This Agreement relates to the processing of personal data supplied by Heriot-Watt University to [….] in relation to the above contract.

The definitions: "personal data" and "processing" are as set out in Parts 1 and 2 of the Data Protection Act, 1998.

The Parties agree to fulfil their obligations under the Data Protection Act 1998 (in particular the eight principles set out in schedule 1 to that Act). Each party warrants and undertakes that it will have in place appropriate technical and organisational measures to protect personal data it shares with the other against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected. Each party has the right to audit processing of shared personal data held by the other party to monitor compliance with the Data Protection Act 1998.

We, […], agree to the following terms & conditions of processing personal data.

1. Personal data provided by Heriot-Watt University for processing in connection with this contract will only be used by responsible officers within […] for the purposes agreed by Heriot-Watt University and will not be transferred to sub-contractors or other third parties without prior consent from Heriot-Watt University.

2. If […] transfers shared personal data to countries outside the EU with prior consent from Heriot-Watt University, transfer contracts must include the standard clauses for data transfers to non-EU countries (7.1.2005) set out in European Commission Decision C(2004)5271.

3. All personal data provided to […] for processing in relation to this contract will be returned to Heriot-Watt University upon written request and/or on completion of contract or securely shredded in accordance with Heriot-Watt University requirements for data management and electronic copies deleted.

4. […] accepts responsibility for keeping all personal data secure, and for applying appropriate security measures for electronic and (or) paper copies of personal data provided by Heriot-Watt University. […….] shall ensure that appropriate technical and organisational security measures are taken against unauthorised or unlawful processing of personal data and against accidental or unlawful loss, alteration or destruction of, or damage or access to, such personal data and against all other unlawful forms of processing of personal data. For the purposes of this paragraph (4), security measures which comply with ISO 27001

POLICY

and ISO 27002 (or any replacement standards relating to data security) for data security shall, unless otherwise notified in an appendix to this agreement by Heriot-Watt University to […….], be deemed appropriate in the circumstances.

5. […] undertakes not to use personal data transferred to it for processing by Heriot-Watt University in presentations, software demonstrations or other training purposes.

6. The Computer Misuse Act stipulates access to unauthorised information is an offence. […] will ensure that all measures have been put in place (e.g.. password protection) to prevent unauthorised access to personal data

7. […] will allow inspection of its premises and systems by Heriot-Watt University's Data Protection Officer or his/her nominee (as necessary) to ensure appropriate security measures are in place.

8. […] will be liable for misuse or breach in use by its staff or contractors of personal data provided by Heriot-Watt University, and shall indemnify Heriot-Watt University against any loss or damage incurred by Heriot-Watt University arising from such misuse or breach.

9. This Agreement imposes no obligation upon […] with respect to personal data which (a) was known to […] before receipt from Heriot-Watt University; (b) is or becomes publicly available through no fault of […] (c) is rightfully received by […] from a third party without a duty of confidentiality; (d) is disclosed by Heriot-Watt University to a third party without a duty of confidentiality on the third party; or (e) is disclosed by […] with Heriot-Watt University's prior written approval. If […] is required by a government body or court of law to disclose the personal data provided by Heriot-Watt University. […] agrees to give Heriot-Watt University reasonable advance notice so that Heriot-Watt University may contest the disclosure, or seek a protective order.

Signed: (on behalf of Heriot Watt University) ……

Print Name: ……

Role: Data Protection Officer

Date ……..

Signed: (on behalf of […]) ……...

Print Name: ……

Role:

Date:……

POLICY

Data Processor to complete and sign two copies and return to
Ann Jones, FOI and Data Protection Officer
Heriot-Watt University
Edinburgh EH14 4AS
Tel: 0131 451 3219 Email: Foi@hw.ac.uk

POLICY

Heriot-Watt University approvals log
Initiator: [name, role]

Data Transfer approvals

Responsible Officer/s

Name	Role	Signature	Date

[
Data Protection Officer [signature, date]

Specific security conditions approved by above on [date] and appended

Fair Processing Notice approved by above on [date] and appended

References

- **Data Protection Act 1998**
  http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1
- **Standard clauses for data transfers to non-EU countries** (7.1.2005) set out in European Commission Decision C(2004)5271.
  http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm
- **The Computer Misuse Act, 1990**
- http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

POLICY

Personal data processing by external suppliers, contractors, agents and partners

Section 1.3: Procurement Services will update the University's Terms and Conditions so the strictures of this Policy are imported into any ensuing contract. For new suppliers, Procurement Services will amend the 'New Supplier Registration Form' to include a signed section for suppliers to document their acceptance to comply.

Section 1.4: Procurement Services will be responsible for completing the procedure with the Data Protection Officer only for those contracts where there is no specific end-user with dedicated responsibility for its management (*e.g.* the Travel Contract). In other cases, the Authorised Contact will be the relevant end user who commissioned the contract. The appropriate officer from the user Department will be responsible for the monitoring and auditing of the Agreement and the contractor, including carrying out stringent checks on the service provider.

Some current and forthcoming contracts which may be caught by this Act include: Travel (in hand); Payroll Bureau; Oracle Support/HR system; Agency Staff; Procurement Card; Cycle-to-Work; ResNet; Leisure Management System; Special Needs/Access to Work; Health Centres; Nursery; SAS.

POLICY