Sample DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

This CCN is being raised to facilitate ELEXONs calculation and management of the Revenue Protection Risk factors when reporting on risk.

As theft is believed to be a large source of erroneous data within Settlement, it is important for ELEXON to carry out a detailed and rigorous analysis of theft using the best available data to ensure that the reporting generated is as accurate as possible.

ELEXON is looking to establish reporting which confirms that all identified theft is correctly settled. To support this ELEXON is requesting access to Electricity Theft Data at an aggregated market-wide, aggregated MPID-level and MPAN-level data of identified theft. ELEXON would like the last three years of Theft data from the TRAS Outcome Files, from April 2016 onwards, or as much as is available, in order to assist in risk evaluation. ELEXON requests a monthly submission of all future TRAS Outcome Files.

A DPIA is required as ELEXON and Electralink both deem an MPAN to be personal data.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

The TRAS will provide data to ELEXON

ELEXON will create a report that reconciles identified theft from TRAS and Data Flows from the DTN that serve the purpose of accounting for theft in settlement. The data will also be used to evaluate the Risk that Revenue Protection has in the GB Energy Market.

ELEXON will store the data on its servers.

Data will be retained for reporting and scoring purposes.

The TRAS (Meters) is the source of the data.

ELEXON will share the data with the GB energy parties that will have previously been notified of the data.

ELEXON understands the high-risk nature of the data it is requesting, however ELEXON has a multitude of similar data available to it and has governance in place to prevent data privacy breaches.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

A list of the Data requested is below, and it contains a Crime Reference Number, although this is not vital to the assessment, it would be advantageous to understand theft cases that are or are not reported to the police. The data collected will be all instances in the month, and data will be provided monthly, and will be retained for reporting and scoring purposes. Individuals should not be affected, the data will be used at a GB Energy Party level. The Data should cover ~~the~~ Great Britain.

Data Block	Field Name
Supply Block	**MPAN / MPRN**
Meter Block	**Meter Serial Number**
Investigation Outcome Block	**Supplier Investigation ID No**
	Theft lead source
	Date Investigation Closed
	Current_investigation_code
	Type of theft
	Crime reference no
	Assessed start date for theft
	Assessed end date for theft
	Assessed losses
	Tampering Code
	Tampering Report Date
	Tampering Report Source
	Security devices fitted

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

ELEXON are the code administrator of the Balancing and Settlement Code and Electralink operate the Theft Risk Assessment Service and are a code administrator for The Distribution Connection and Use of System Agreement. GB Energy Parties are signatories of both ELEXON and DCUSA.

Parties will receive their TRAS data report before or in conjunction with ELEXON. ELEXON will then reconcile the identified theft within, with any D0019 adjustments, sent by the DC, to those meters to ensure theft is correctly Settled, as outlined in BSCP504 - 3.6. ELEXON already has access to D0019 flows sent across the DTN.

This reconciliation report will then be sent to the parties for their attention. Parties expect Code administrators to work together for the improvement of the GB Energy Market.

No information regarding individuals' vulnerability status will be shared with ELEXON. There are no prior concerns with ELEXONs access to MPAN-level data.

ELEXON has its ISO27001 GDPR rating.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
ELEXON is requesting access to the data to produce reporting which will be delivered to GB Energy Parties. The intent of the reporting is to assess the reconciliation of theft data, improve ELEXONs understanding of the Revenue Protection Risk, and to provide information to Parties on outstanding reconciliation to be undertaken. This should result in an increased accuracy of Settlement and Trading Charges.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

ELEXON are the code administrator of the Balancing and Settlement Code (BSC), GB Energy Parties are signatories of the BSC. The processing will confirm identified cases of Electricity theft, which ELEXON can use to search for theft reconciliation. The TRAS is a mechanism for the identification and reporting of energy theft, and it is therefore the best source for this data.

ELEXON has outlined the scope for which the data will be used. This covers the reporting, risk analysis, and understanding of the GB Energy Market, and ELEXON will put governance in place to prevent the misuse of the data. Elexon will ensure data quality by introducing validation checking into the reporting. ELEXON will give parties a reconciliation report of their TRAS data, and the data flows the party sends to account for energy theft.

ELEXON will introduce Local Working Instructions (LWIs) and training to ensure the protection of rights and the processors remain compliant, and there is no transfer of data outside of stated in scope.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
ELEXON match MPAN numbers from the data to personal information of individuals available on ECOES Systems.	Possible	Minimal	Low
ELEXON provide an energy party with another party's information.	Remote	Minimal	Low
Reporting errors results in misrepresentation of a party's theft reconciliation position.	Possible	Minimal	Medium

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
ELEXON match MPAN numbers from the data to personal information of individuals available on ECOES Systems.	LWIs and training to ensure matching is not undertaken.	Eliminated reduced accepted Reduced	Low medium high Low	Yes/no
ELEXON provide an energy party with another party's information.	ELEXON will include the report in a reporting pack, which would be checked to ensure all reports are intended for the receiving party.	Eliminated	Low	
Reporting errors results in misrepresentation of a party's theft reconciliation position.	Consultation process prior to implementation for parties to challenge ELEXON reporting Data validation checks in place. Automation of reporting.	Reduced	Low	

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		

This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA