12 May, 2026

Data Repository User Group

Meeting One

ELEXON

Introduction and Agenda

ELEXON

Agenda

What we'll cover today…

1

Design overview

2

User Interface and data sets

3

Legal Basis

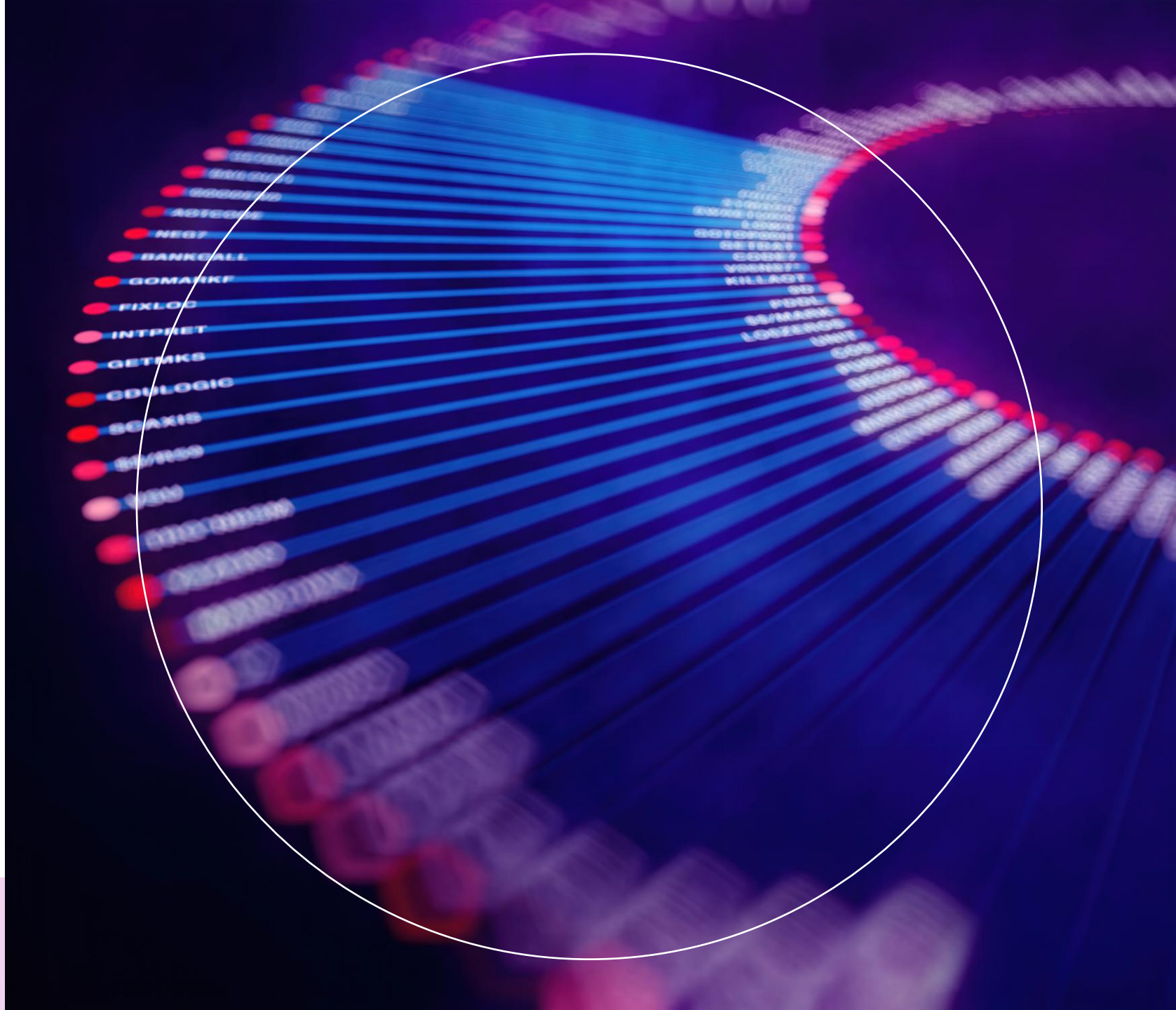
4

Privacy Policies

ELEXON

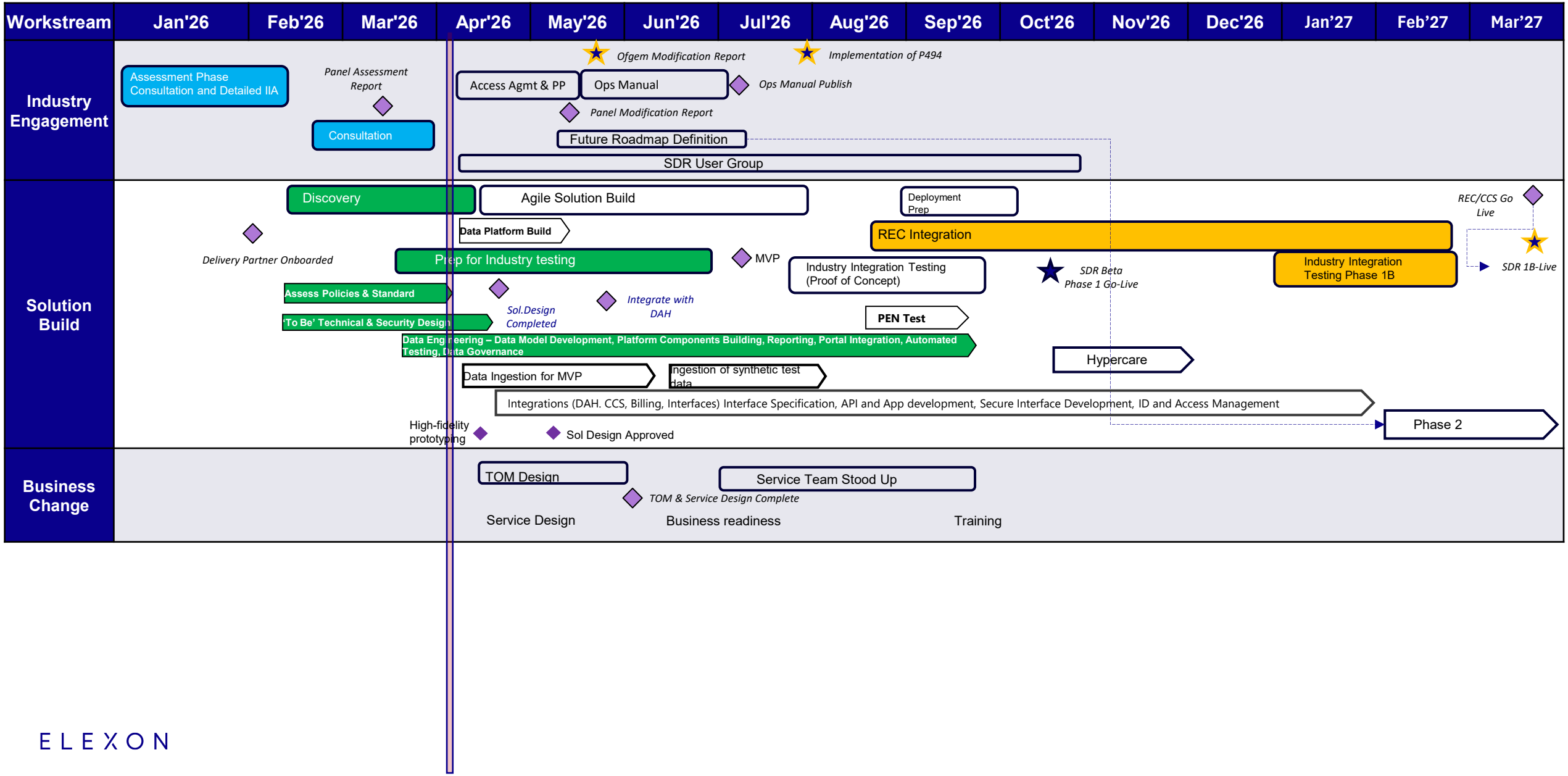
02

Design Overview



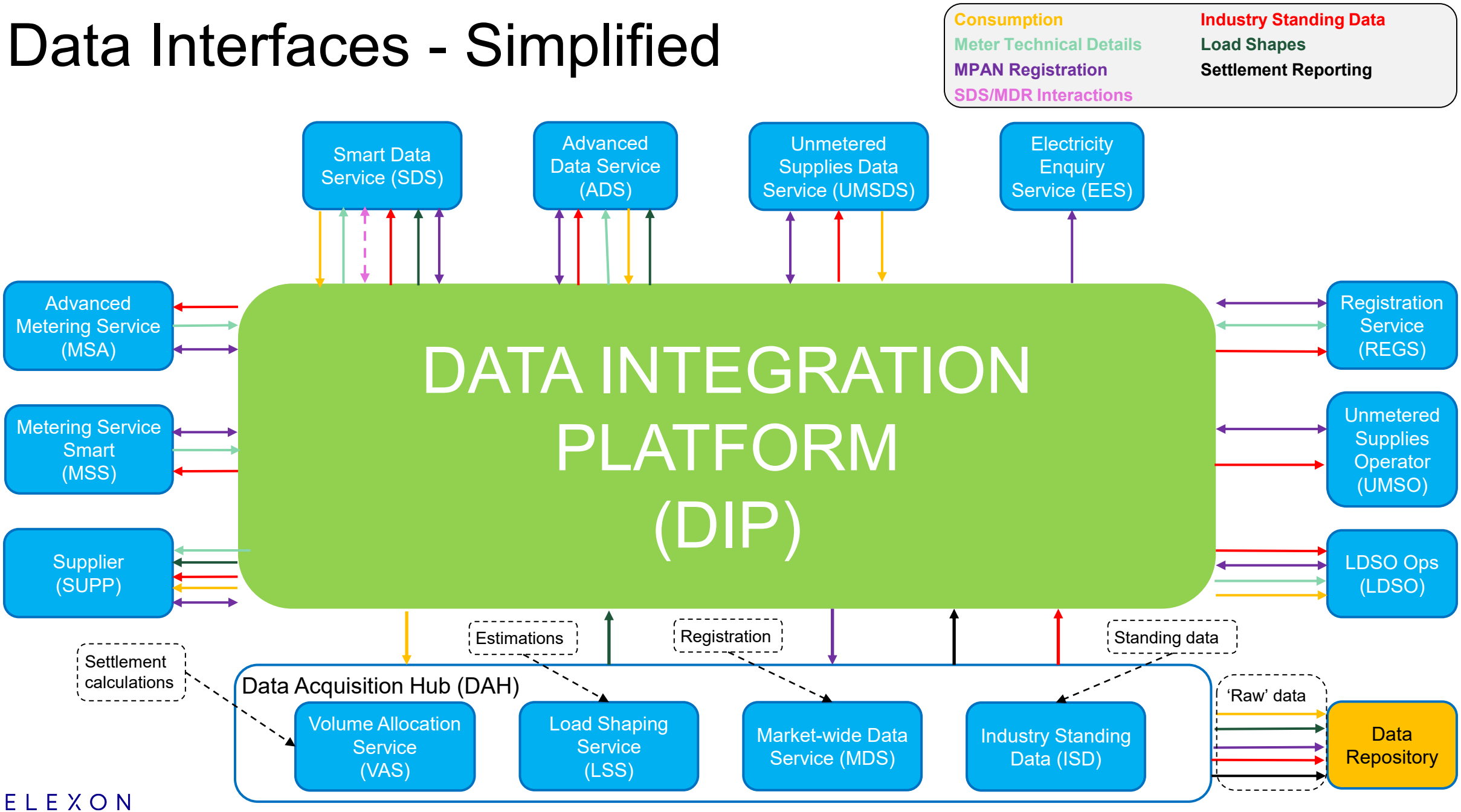
ELEXON

Programme Roadmap



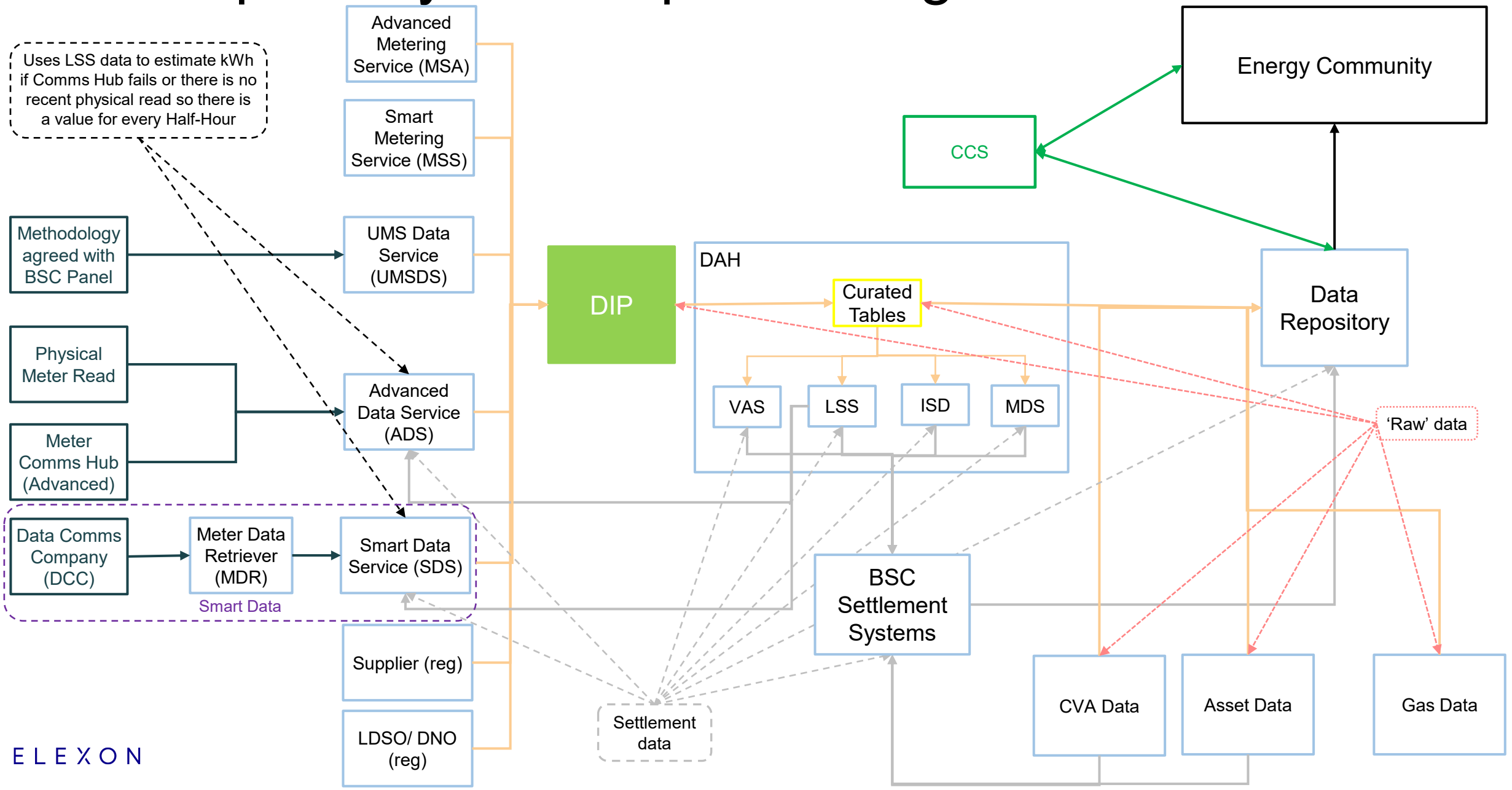
ELEXON

Data Interfaces - Simplified



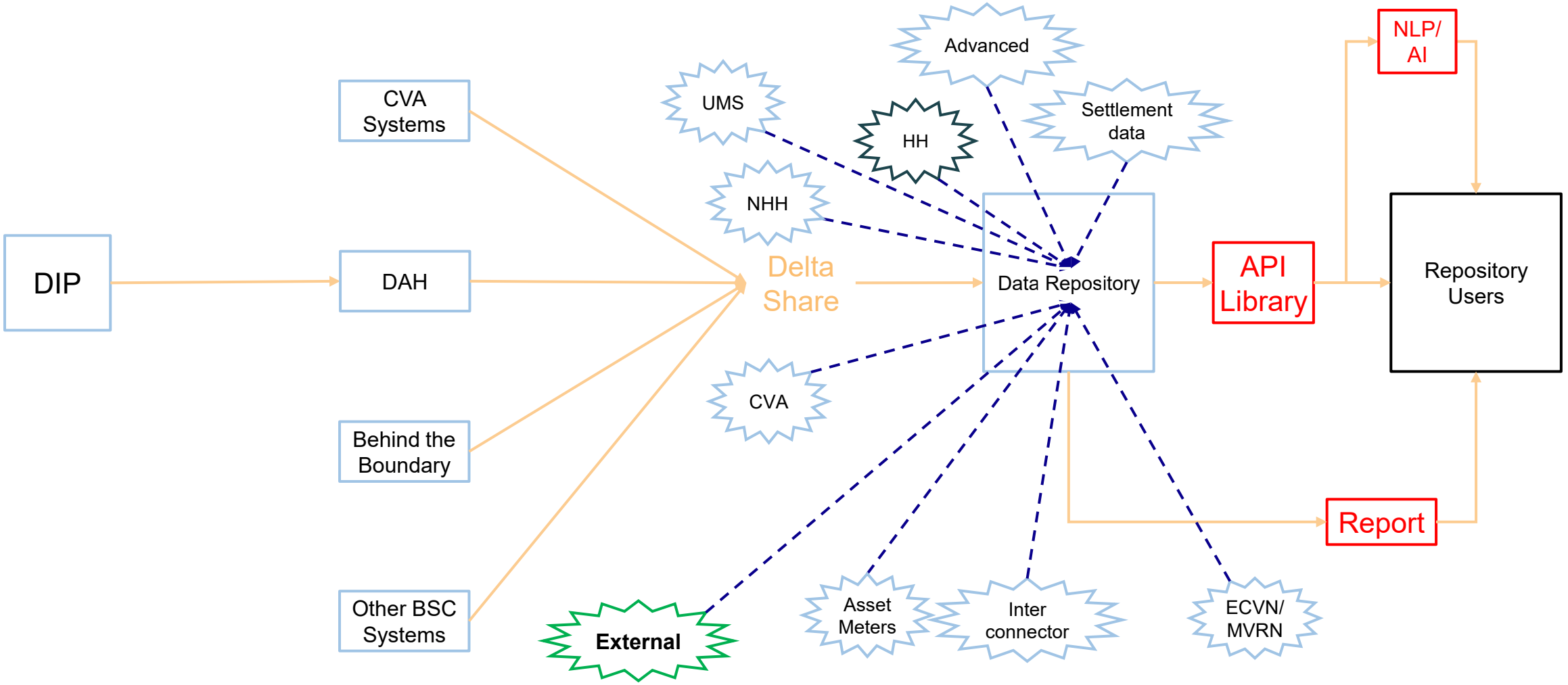
ELEXON

Data Repository– conceptual design end state

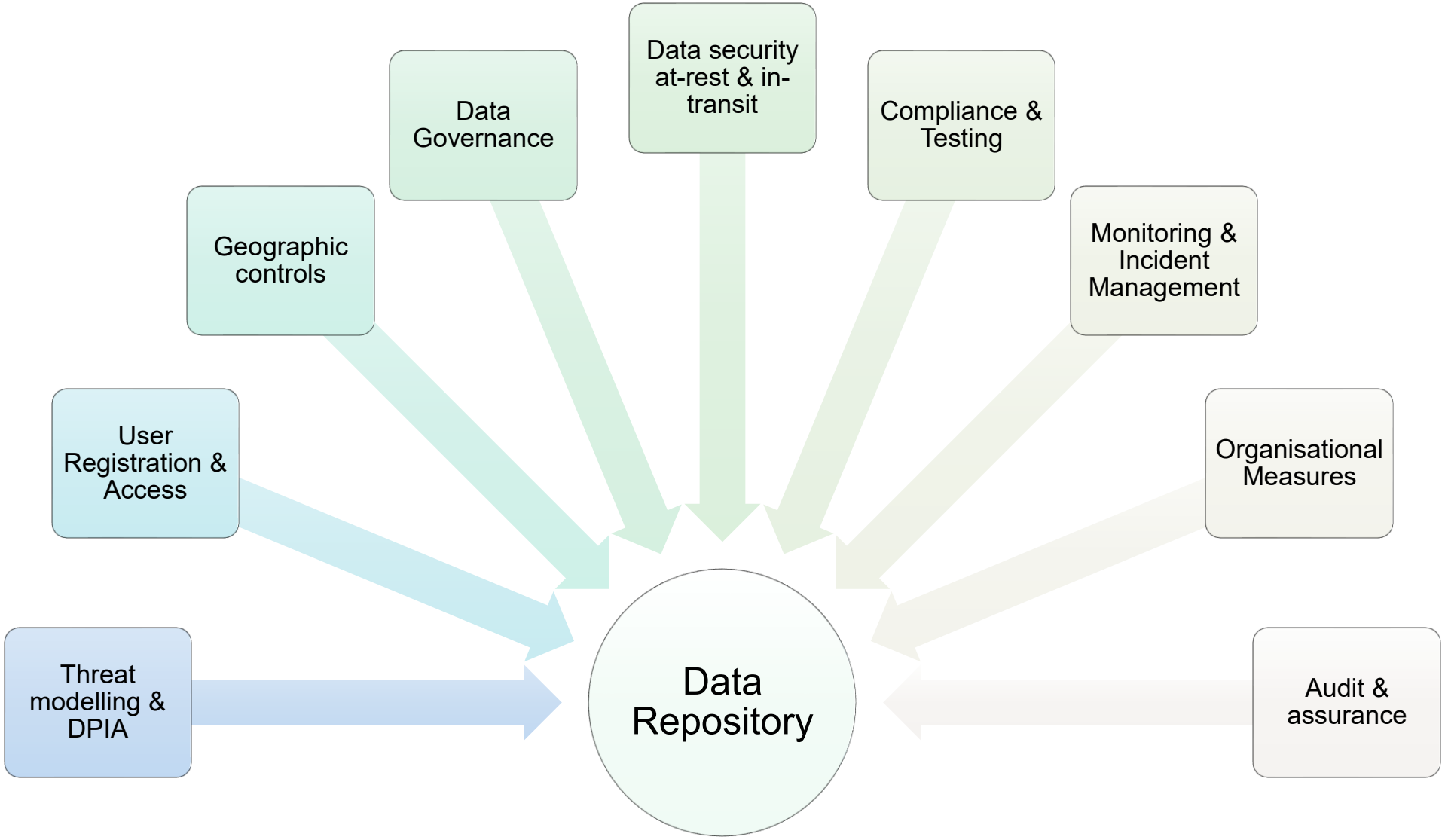


ELEXON

Conceptual high-level design – end state



Designing the Data Repository

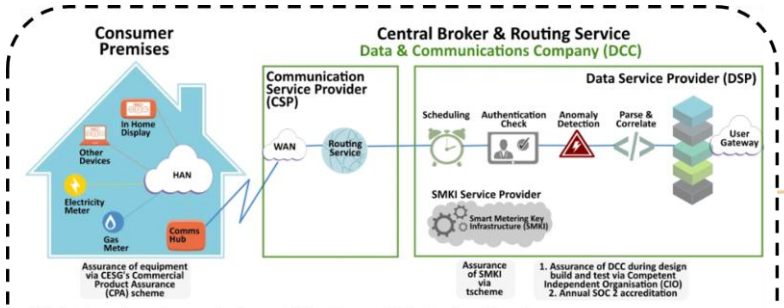


Smart metering security trust model

Secure Software Development Life Cycle

- Legal, statutory, regulatory, contractual requirements
- Threat modelling – business and technical architecture
- Secure design
- Secure Coding
- SAST, DAST, SCA, pen testing
- Integration with SOC

Secure Config



High level system design of the Smart Metering System (taken form NCSC website)

Meter Data Retriever (MDR) → Smart Data Service (SDS) → DIP → DAH → SDR

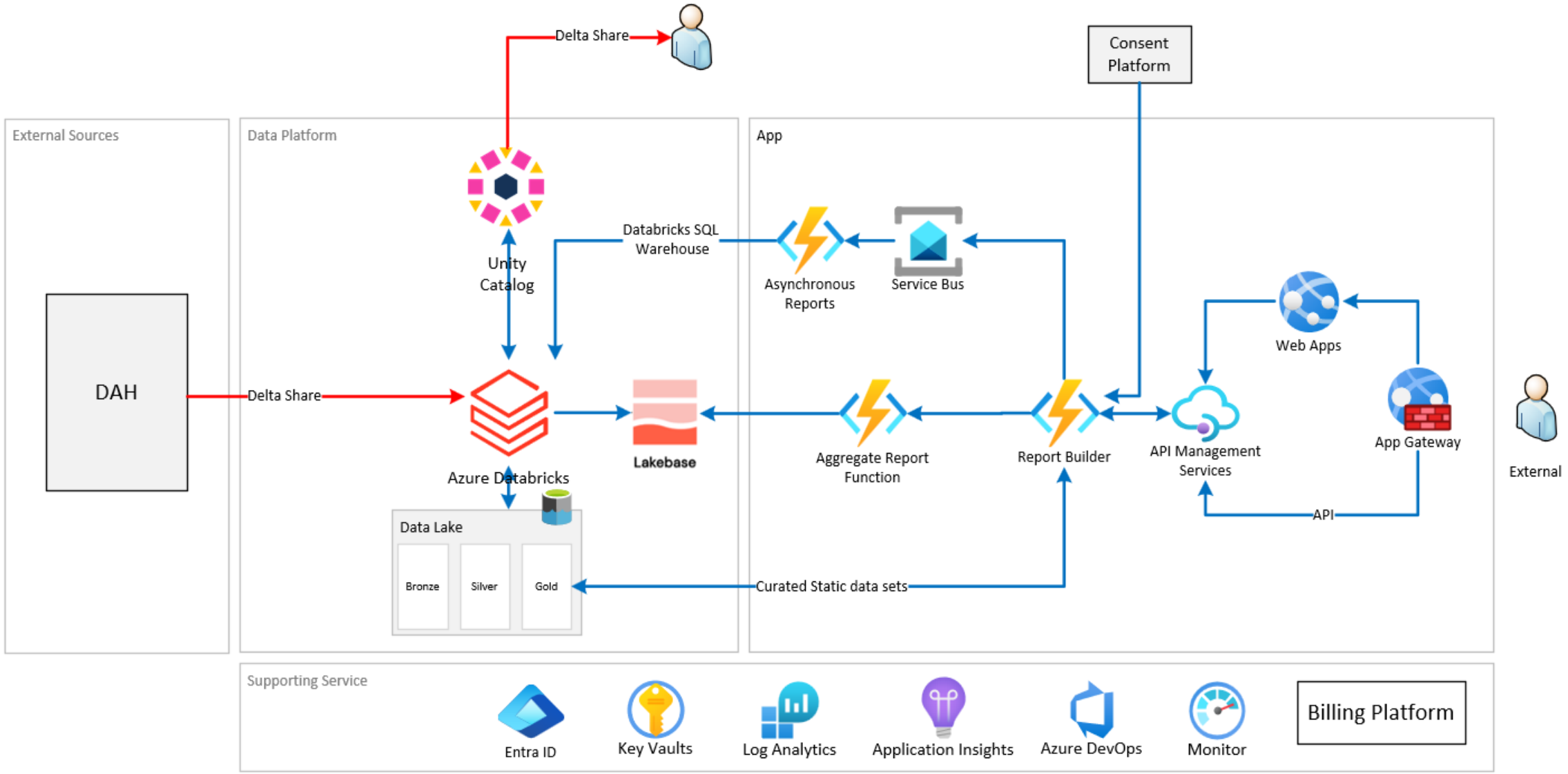
Secure Coding

Security - Operations

- Education and Training
- Threat intelligence Scanning
- Sentinel – Security monitoring (SOC)
- Vulnerability and patching
- ISO27001
- Supplier Assessment

ELEXON

Data Repository High Level Design



Data Repository Technical Architecture

SDR Users

Elexon Operator

WEB SECURITY — App Gateway + WAF + (Secure coding – input validation, output encoding, http policy, Infrastructure-as-Code)

API SECURITY — Azure APIM (OAuth 2.0 · JWT validation – scopes and claims · rate limiting · mTLS · API versioning · Secure Coding)

Network — Custom NSGs · network segmentation · private links · VNETs · private subnets

Infrastructure and platform — secure configs · role-based access control · vulnerability scanning with Defender · Access control for control plane and data plane · CosmosDB · Event Bridge · Service Bus · Key Vaults

Cryptography — cipher suites (NCSC recommended) for transport layer, public keys and private keys, certificate authority, certificate lifecycle

IDENTITY & AUTH — Entra ID (RBAC · PIM · SCIM) · Entra External ID (CIAM) · CCS (Consents) · Managed Identity

Support systems — Code base · CI/CD pipelines · images and image registry · RBAC for ADO · Application Insights · Log Analytics

DATA PLATFORM – SECURITY and GOVERNANCE

ADLS Gen2 (Bronze·Silver·Gold) · Databricks SQL Warehouse · Purview and Unity Catalog (governance · lineage · column masks) · Delta Sharing (ext. consumers) · derisking malicious profiling · access control

Web portal security | API security | Network | Infrastructure and platform | Cryptography | Identity | Support systems | Data

Security Operations – Monitoring, Vulnerability and patching, threat monitoring, Security incident management process, BC/DR, change management, scans, supplier assessments, ISO27001

03

User Interface and datasets

ELEXON

User interviews

“Not being too cluttered, being clearly labelled, having a title, having axes.”

“Simpler the better, not making it complex for the sake of it.”

“What we try to avoid is websites that are so blisteringly complex that a new entrant just gives up.”

“We don’t have access to this data today — so access to it is the excitement in itself.

“There should be a way of being alerted that things are changing.”

ELEXON

Identifying personas and user journeys

Market Analyst

Riley Morgan

Time in role	**11 years**
Gender	**Female**
Age	**28 years**
Accessibility	**N/A**

About

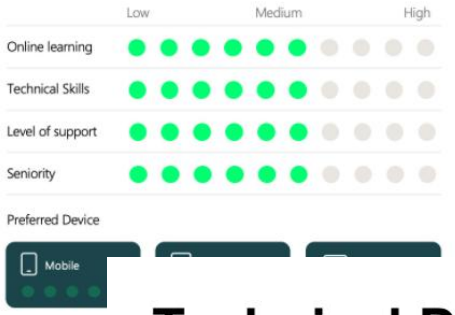
Riley Morgan is a market or commercial analyst working in the energy sector, such as a supplier, network operator, consultancy, or market intelligence role. They use aggregated energy data to understand market dynamics, analyse trends, and support forecasting and strategic decision-making. Riley focuses on interpreting data to inform commercial and market-facing insights rather than working with raw datasets.

ELEXON

Goals

- Build a clear picture of how the energy market is changing over time.
- Use trusted aggregated data to support forecasts and scenario thinking.
- Identify emerging trends, risks, or opportunities early enough to act on them.
- Provide evidence that informs strategic, commercial, or investment decisions.
- Communicate market insights confidently to stakeholders who rely on clear signals, not raw data.

Professional profile



Concerns

- Data that lacks enough context to explain why trends are changing.
- Uncertainty about how complete, consistent, or representative the data is.
- Difficulty making fair comparisons across time periods or market segments.
- Risk of drawing conclusions from data that is outdated or methodologically unclear.

Needs

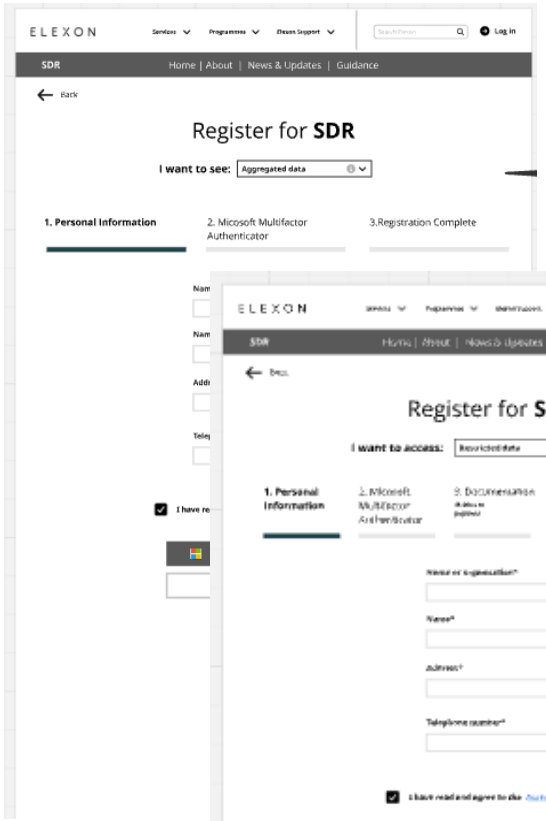
- Aggregated, market-level data that is consistent and comparable over time.
- Clear explanations of coverage, assumptions, and known limitations.
- Visual summaries or indicators that highlight meaningful changes and patterns.
- Confidence that the data is suitable for forecasting and market analysis.

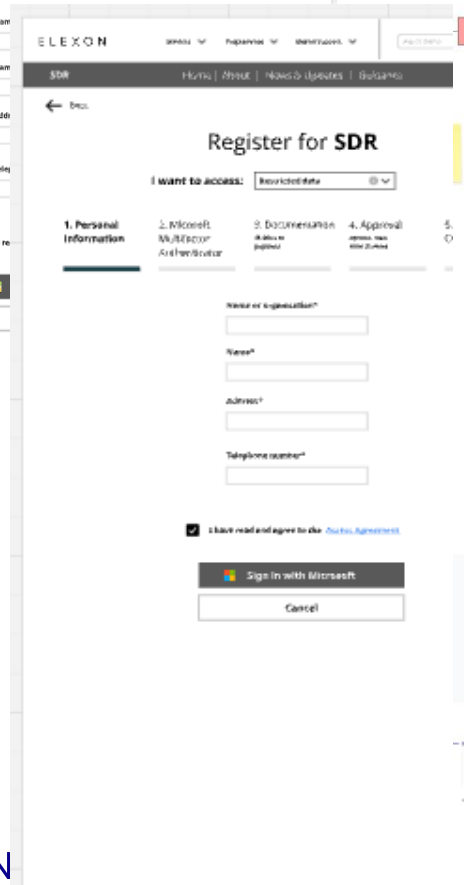
Technical Developer User Journey

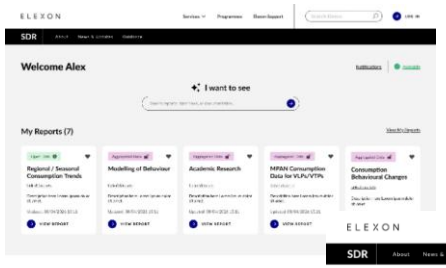
	User Actions & Touchpoints	Goals/Needs	Pain Points / Challenges	Opportunities & Supporting Features
Discover	Explores SDR developer portal, reviews API documentation, data catalogues, quick-start guides, and sample code to assess suitability for integration.	Understand available APIs and datasets quickly; confirm data coverage, structure, and stability; plan an efficient integration approach.	Poorly structured documentation; unclear data definitions; fragmented information; time pressure to start development.	Clear developer portal, searchable API documentation, well-documented schemas, sample responses, and consolidated access to datasets.
Access	Registers via self-service developer portal, configures authentication (API keys or OAuth), tests endpoints using tools like Postman.	Fast, self-service access; secure authentication; clear understanding of permissions and rate limits.	Delayed approvals for certain data; unclear auth flows; permission errors without explanation.	Self-service onboarding, standard OAuth/API key setup, clear permission messaging, sandbox or test environments.
Analyse	Builds and tests automated data pipelines using SDR APIs, handles pagination, error handling, and data transformation.	Reliable, performant data ingestion; automation with minimal manual intervention; clear data context.	Breaking API changes; performance issues; lack of transparency in aggregated data	Versioned APIs, change logs, bulk and incremental endpoints, metadata and data quality indicators.
Maintain	Monitors integration health, responds to alerts, reviews release notes, updates integrations as APIs evolve.	Stable integrations; early warning of issues; predictable change management.	Unexpected breaking changes; slow or unclear support responses; lack of visibility into platform issues.	Monitoring dashboards, proactive alerts, advance deprecation notices, responsive technical support.

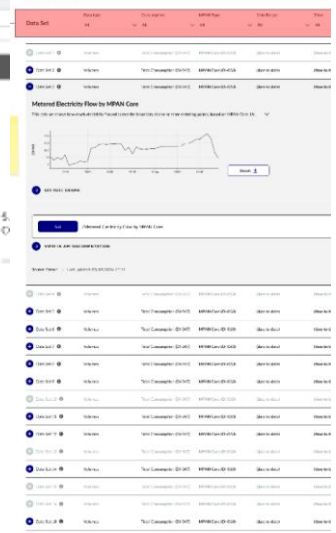
ELEXON

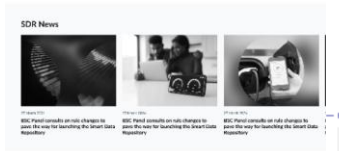
Wireframes and designs

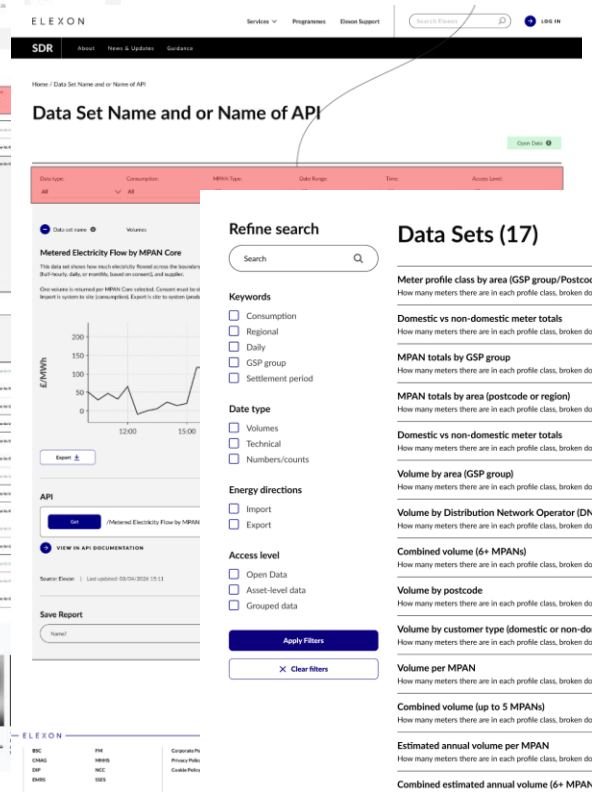




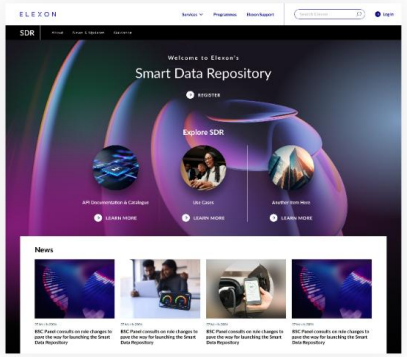


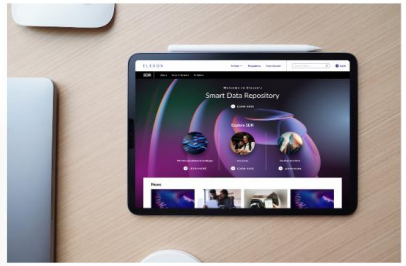






3.
Wild Child





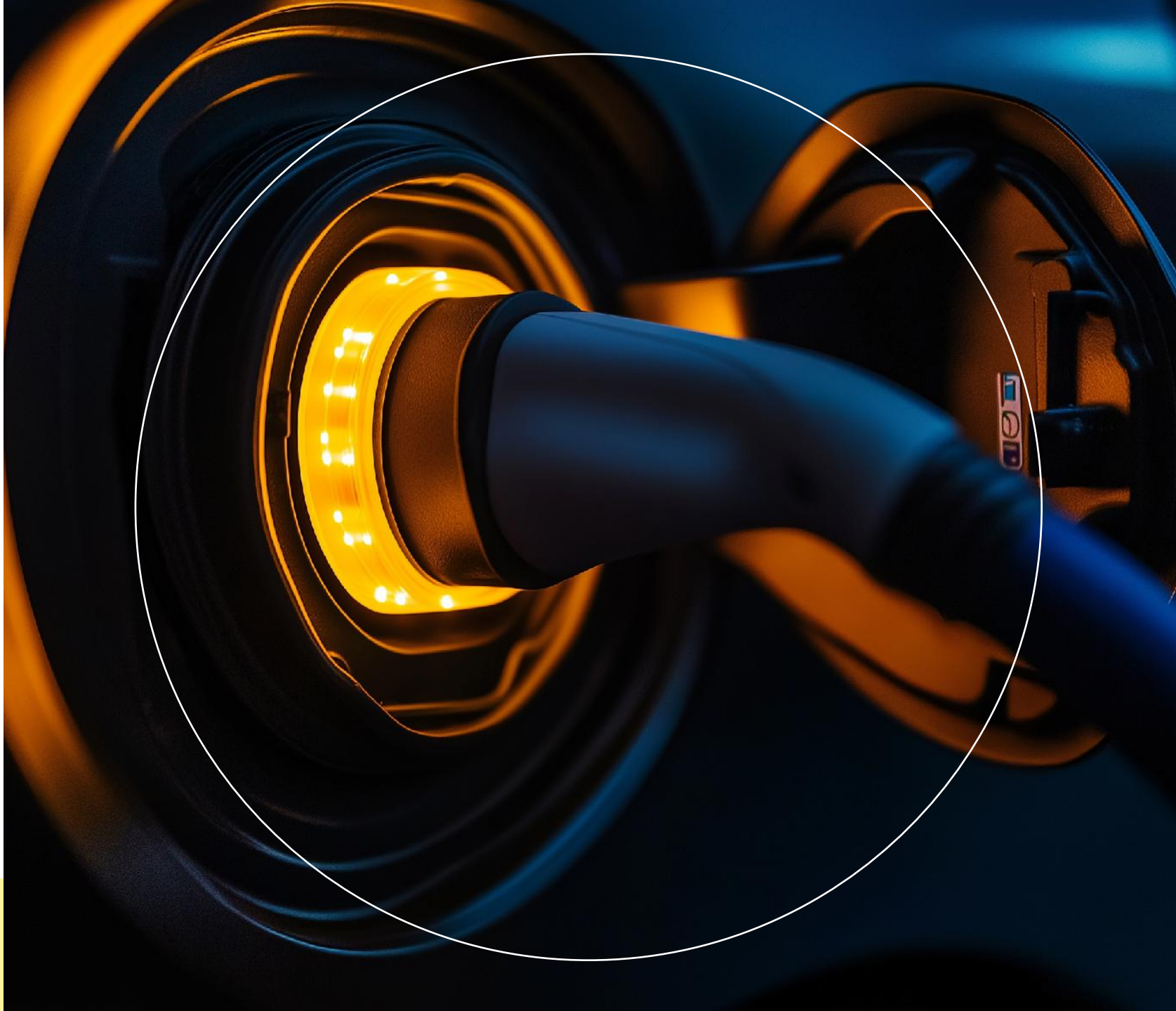
ELEXON

Data Sets and Use Cases

Category	Data Set ID	Data Set name	What this dataset gives you
Volumes	DS01	Volume per MPAN	How much electricity has been used or sent back to the grid at each metering point (MPAN) over a given period
Volumes	DS02	Combined volume (up to 5 MPANs)	The total amount of electricity used or sent back to the grid across up to five meters (MPAN) over a given period, with all meters added together into one combined figure.
Volumes	DS08	Combined volume (6+ MPANs)	The total amount of electricity used or sent back to the grid across six or more meters (MPAN) over a given period, with all meters added together into one combined figure.
Volumes	DS03	Estimated annual volume per MPAN	The estimated amount of electricity each meter (MPAN) is expected to use or send back to the grid over a year.
Volumes	DS05	Combined estimated annual volume (up to 5 MPANs)	The total estimated amount of electricity that up to five meters (MPAN) are expected to use or send back to the grid over a year, with all meters added together into one figure.
Volumes	DS04	Combined estimated annual volume (6+ MPANs)	The total estimated amount of electricity that six or more meters (MPAN) are expected to use or send back to the grid over a year, with all meters added together into one figure.
Volumes	DS06	Volume by area (GSP group)	How much electricity has been used or sent back to the grid in a given postcode, or across a wider region built from multiple postcodes, over a chosen period.
Volumes	DS07	Volume by Distribution Network Operator (DNO)	How much electricity has been used or sent back to a Distribution Network Operator's network over a chosen period.
Volumes	DS09	Volume by postcode	How much electricity has been used or sent back to the grid in a specific postcode, or across a wider region made up of multiple postcodes, over a chosen period.
Volumes	DS17	Volume by customer type (domestic or non-domestic)	How much electricity has been used or sent back to the grid, split by domestic and non-domestic customers, over a chosen period.
Technical	DS10	Meter technical details	Key technical attributes for a specific metering point (MPAN), including identifiers and installation date.
Technical	DS11	Meter profile class by area (GSP group/Postcode)	How many meters there are in each profile class, broken down by GSP group or by postcode.
Numbers/counts	DS12	Meter type totals	How many meters of each meter type there are, broken down by GSP group or by postcode
Numbers/counts	DS13	MPAN totals by Distribution Network Operator (DNO)	How many metering points (MPANs) there are for one or more Distribution Network Operators.
Numbers/counts	DS14	MPAN totals by GSP group	How many metering points (MPANs) there are in one or more GSP groups.
Numbers/counts	DS15	MPAN totals by area (postcode or region)	How many metering points (MPANs) there are in a specific postcode, or across a wider region made up of multiple postcodes.
Numbers/counts	DS16	Domestic vs non-domestic meter totals	How many domestic and non-domestic meters there are, broken down by postcode/region, GSP group, Distribution Network Operator, or supplier.

04

Legal bases



ELEXON

Flow of data – legal perspective

Supplier collects – License obligations

Gives to Elexon (via DIP) for Settlement purposes - BSC obligation and license conditions

Elexon carries out Settlement process – DAH & Other Systems e.g. Settlement Administration Agent (SAA) and Energy Contract Volume Allocation Agent (ECVAA) – as data processor

DAH to Repository for reporting and sharing - API/Reports – Elexon now moves into data controller role, where we need a lawful basis to process said data

Lawful basis – Public Task (GDPR Article 6(1)(e))

- Where a specific task in the public interest is laid down by law
- Applies even if the organisation performing it is not itself a public authority
- The ICO guidance explicitly says private companies can rely on Public Task

- Public Task cannot be used where the controller is subject to a specific legal duty to hold, evidence or retain data;
- Legitimate Interests is used only where neither Legal Obligation nor Public Task fully applies and in limited circumstances;
- Legitimate Interests will apply to anonymized and/or aggregated analytics supporting: innovation; flexibility; market development

Lawful basis processing

Processing activity	Detailed description	Purpose	Lawful basis	Necessity justification	Safeguards / conditions (incl. national infrastructure considerations)	Role	Responsibility
Settlement processing (pre-SDR)	Data processed within central BSC systems (e.g. DAH) for settlement purposes	Settlement, validation, aggregation and reconciliation	Legal obligation (Article 6(1)(c) applicable to suppliers)	Necessary to fulfil statutory settlement obligations under the BSC and Electricity Act; processing cannot be carried out without consumption data.	Encryption of data in transit and at rest; secure ingestion pipelines; network segmentation.	Processor (BSCCo, to the extent it processes personal data on behalf of BSC Parties)	Suppliers (and other BSC Parties) responsible as controllers for data accuracy and submission; BSCCo/BSC Agents responsible for processing in accordance with BSC instructions
Receiving data into the SDR	Elexon receives data (including MPAN-level consumption data) from systems such as DAH	To establish and operate the SDR	Public task	Necessary to establish a centralised, secure repository (SDR) to govern access and reduce fragmented and higher-risk data handling across the market.	Strict access controls (RBAC/ABAC); strong authentication for APIs and access controls that mitigate OWASP Top 10 risks for APIs; network segmentation for resources consuming data from systems such as DAH	Controller	BSCCo is responsible for data from the point of ingestion into SDR; upstream controllers responsible for data accuracy and completeness prior to transfer
Storing data	Data is securely stored within the SDR	Enable access and governance	Public task	Necessary to securely store and retain data to meet audit, assurance, and dispute resolution requirements, including defined retention periods.	Purpose limitations enforced through onboarding; contractual controls; system-level access restrictions; retention controls.; encryption of data at rest with NCSC recommended algorithms	Controller	BSCCo responsible for security, integrity and retention

Lawful basis processing

Processing activity	Detailed description	Purpose	Lawful basis	Necessity justification	Safeguards / conditions (incl. national infrastructure considerations)	Role	Responsibility
Processing data	Data is organised, validated and prepared for use	Ensure data quality and usability	Public task	Necessary to structure, validate and maintain data quality to ensure accuracy, integrity, and reliability of market processes.	Input Data validation controls; output data encoding; reconciliation checks; audit trails; role-based access controls ensuring processing is limited to authorised functions.	Controller	BSCCo responsible for processing integrity within SDR
Aggregating data	Data transformed into aggregated/anonymised datasets	Enable safe use and disclosure	Public task	Necessary to aggregate data to support BSC functions; where data is fully anonymised where no individual is identifiable, it falls outside the scope of UK GDPR.	Anonymisation and aggregation techniques; minimum aggregation thresholds (k-anonymity); suppression of small cells; bucketing of data to mitigate re-identification of data subjects; validation of data that is rendered to the user; controls to prevent re-identification and inference of individual households or critical energy infrastructure patterns.	Controller	BSCCo responsible for anonymisation and aggregation standards
Providing aggregated data	Aggregated data shared with users	Market transparency	Public task (where data remains personal data); not applicable where data is fully anonymised	Necessary for the performance of Elexon's functions under the BSC to provide aggregated data for defined transparency, regulatory oversight and market insight purposes,	Disclosure control processes; aggregation thresholds; statistical disclosure limitation techniques; review mechanisms to prevent inference of individuals or sensitive	Controller	BSCCo responsible for lawful disclosure and safeguards

Lawful basis processing

Processing activity	Detailed description	Purpose	Lawful basis	Necessity justification	Safeguards / conditions (incl. national infrastructure considerations)	Role	Responsibility
				where no personal data is disclosed.	grid/infrastructure locations.		
Providing consumer-level data	MPAN-level data shared with authorised users	Enable authorised access	Public task	Necessary for the performance of Elexon's functions under the BSC, where provision of MPAN-level data is required for defined and authorised use cases that cannot reasonably be fulfilled using aggregated or anonymised data.	CCS controls governing access permissions, including mechanisms for consumer choice where applicable, with real-time validation and revocation handling; strict role-based access controls based on designed and agreed business justification; audit logging and immutable logs; monitoring of access; safeguards to prevent inference of household behavior or sensitive infrastructure patterns.	Controller noting that certain processing activities relating to access and disclosure are governed by external consent and permission frameworks, such as CCS, and may be subject to those frameworks)	(BSCCo responsible for lawful disclosure, access controls and alignment with access control mechanisms (e.g. CCS) and SDR Rules
Access control and governance	User onboarding, permissions and access control	Ensure secure access	Public task	Necessary to implement access controls and governance to ensure only authorised users access appropriate datasets.	RBAC/ABAC based on job requirements; MFA; user accreditation and onboarding checks; periodic re-certification; purpose limitation enforcement; segregation of duties.; least privilege	Controller	BSCCo responsible for ensuring only authorised access
System monitoring	Monitoring usage and performance	Operational assurance	Public task	Necessary to monitor system usage and performance to detect	Continuous monitoring (SIEM/SOC); anomaly detection; alerting for	Controller	BSCCo responsible for system oversight and compliance

Lawful basis processing

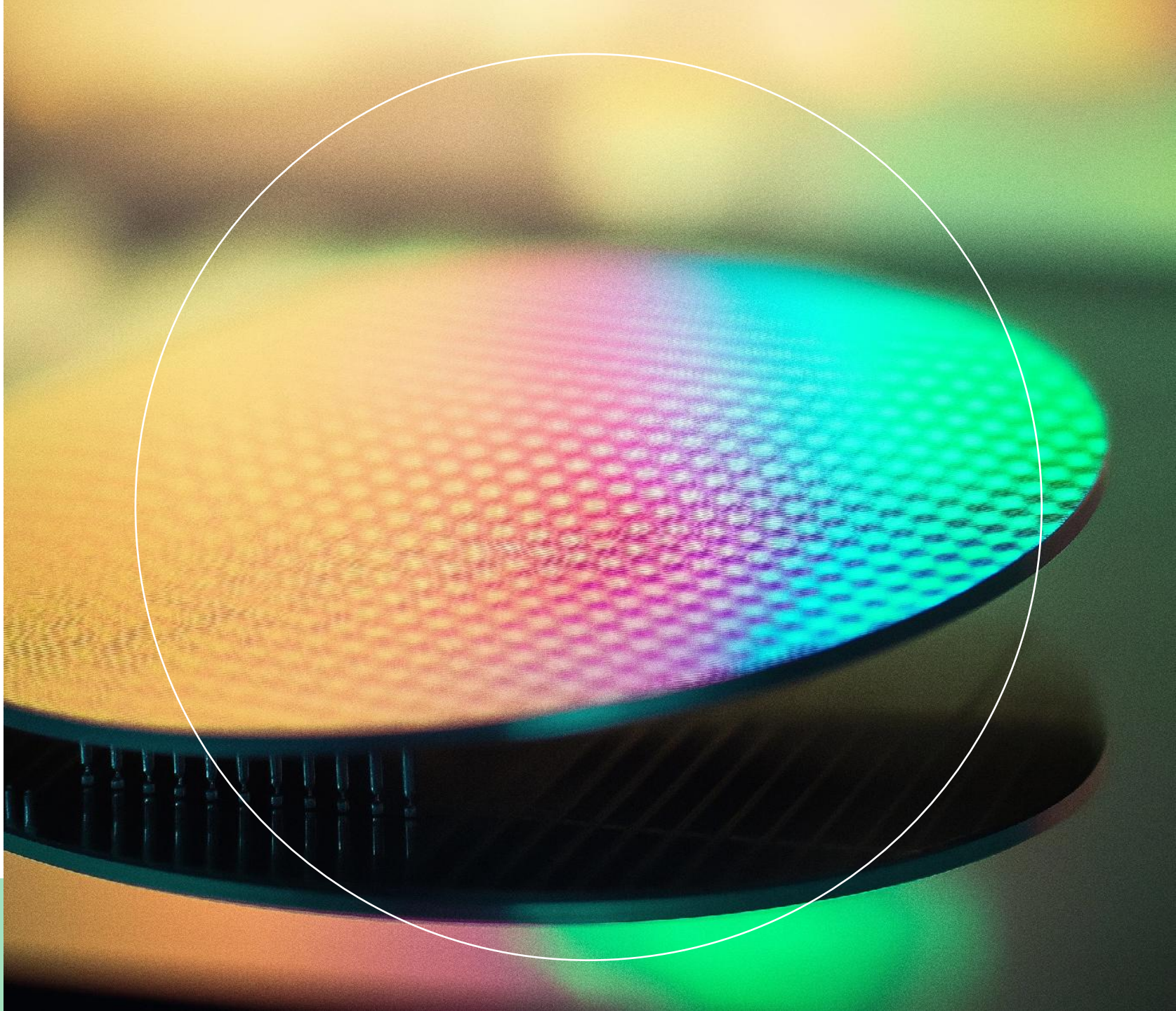
Processing activity	Detailed description	Purpose	Lawful basis	Necessity justification	Safeguards / conditions (incl. national infrastructure considerations)	Role	Responsibility
and reporting				misuse, ensure security, and maintain operational integrity.	unusual access patterns or bulk extraction; incident response processes; comprehensive logging.		
Innovation use (explicitly defined and governed under the BSC and form part of Elexon's functions)	Controlled access for analytics/services	Supporting defined BSC functions and use cases relating to market development and system improvement	Public task	Necessary for the performance of Elexon's functions under the BSC, where access to granular consumption data is required for use cases that support system operation, settlement, authorised under the BSC framework, and cannot reasonably be fulfilled using aggregated or anonymised data	Role-based access control based on designed and agreed business justification; limited access; contractual restrictions; monitoring of usage; controls on bulk extraction; safeguards to prevent misuse for profiling, exploitation, or inference of critical infrastructure vulnerabilities.	Controller	BSCCo responsible for ensuring use aligns with SDR rules
Aggregated data for research	Sharing aggregated and/or anonymised data	Market development	Not applicable (where data is fully anonymised, otherwise Public Task where data remains personal data	Not applicable where data is fully anonymised	Secure API design: APIs built with secure coding; OWASP top 10 risks for APIs mitigated and tested; penetration testing; protection against attack vectors (e.g. man-in-the-middle, credential compromise, privilege escalation);	Controller (where processing involves personal data)	BSCCo responsible for ensuring data is non-identifiable

Lawful basis processing

Processing activity	Detailed description	Purpose	Lawful basis	Necessity justification	Safeguards / conditions (incl. national infrastructure considerations)	Role	Responsibility
					anonymisation assurance processes.		
Data protection compliance	Audit, breach handling and compliance activities	Legal compliance	Legal obligation	Necessary to comply with legal obligations under UK GDPR, including audit, DSAR handling, and breach response.	Alignment with recognised security standards (e.g. ISO 27001, NCSC guidance); encryption of data at rest with NCSC recommended algorithms DSAR identity verification controls; secure delivery mechanisms; breach response procedures.	Controller	BSCCo responsible for GDPR compliance within SDR, including breach assessment and notification
Internal system improvement	Internal analytics and improvements	System performance	Legitimate interests (limited)	Necessary to improve system performance, resilience, and security through internal analytics, using limited and proportionate data. Documented through a Legitimate Interest Assessment (LIA).	Data minimisation; role-based access controls based on job description, segregation of duties and least privilege; restricted internal access; automated deletion/anonymisation controls; legal hold governance; monitoring of internal use.; network segmentation to prevent lateral movement	Controller	BSCCo responsible for ensuring such processing is proportionate and does not override data subject rights

05

Privacy Policy



ELEXON

Supplier compliance under SLC47

1

Data Collection
Suppliers collect and submit consumption data under SLC 47 and BSC obligations
Data is obtained for settlement purposes in accordance with licence conditions

2

SLC 47 and GDPR
The SLC 47 notice/opt-out mechanism:
is a regulatory construct
does not constitute consent under UK GDPR

3

Data Submission
Submission of data into BSC systems:
is mandatory under the regulatory framework
does not constitute onward disclosure by Suppliers

4

Data Repository Interaction
SDR processing is carried out by Elexon as an independent data controller
Based on Public Task (Article 6(1)(e)) under the BSC

ELEXON

Practical considerations for Suppliers

Suppliers do not need to change their core processes — they continue to collect and submit data for settlement as they do today.

Continue business as usual

- Collect and submit consumption data under SLC 47/BSC obligations
- Continue relying on legal obligation (Article 6(1)(c))
- There is no change to data collection, submission processes, or settlement flows

Update privacy notices (main action – more detail in Operations Manual – see next slide)

- Suppliers will need to update their privacy notices to explain that data is processed within the SDR
- This is the only real change for most suppliers

Align with CCS (where relevant)

- this does not change lawful basis - the CCS is for the consumer to consent to access to their personal data

Continue to engage with us

- Participate in SDR user group discussions

Privacy Notice updates – further refined in Operations Manual

We collect and use your electricity consumption data, including half-hourly smart meter readings, to provide our services and to meet our regulatory obligations.

As part of the operation of the electricity market in Great Britain, your data is shared with Elexon Limited ("Elexon"). Elexon is responsible for ensuring the electricity market operates correctly, including calculating settlement and maintaining system balance. When carrying out these activities, Elexon processes data on behalf of the market in accordance with the Balancing and Settlement Code.

Elexon also operates a central system called the Smart Data Repository (SDR). The SDR is a regulated platform, established under the Balancing and Settlement Code and approved by Ofgem. It stores and manages electricity data to support settlement, system monitoring, and other regulated activities.

Within the SDR, Elexon is responsible for how data is managed and made available in line with regulatory requirements. For more information about how and why Elexon processes your data, please see the Elexon Privacy Policy.

In some circumstances, your data may be shared with authorised third parties (for example, to provide services such as energy insights or switching support). This will only happen where you have given your consent through the Consumer Consent Solution (CCS), operated by the Retail Energy Code Company (RECCo). The CCS allows you to control who can access your data, for what purpose, and for how long. You can withdraw your consent at any time.

The SDR is not a commercial data marketplace. Your data is only shared in line with regulatory requirements and data protection legislation.

Thank you