

MEMORANDUM OF UNDERSTANDING

between the

Jersey Data Protection Authority/Information Commissioner

and

Jersey Cyber Security Centre

Contents

1. Definitions	3
2. Recitals	4-6
3. Purpose and principles	7
4. Liaison	7-8
5. Scope of co-operation	8-9
6. Assisting and influencing improvements in cyber security	9
7. Information sharing	9-10
8. The JCSC supporting the JOIC's own cyber security	10
9. JDPA supporting JCSC's own data protection	10
10. Deconfliction between the JCSC and JDPA in relation to incident management	10-11
11. No obligation to meet requests	11
12. Contact points	11
13. Confidentiality	12
14. Retention and disposal of information	12-13
15. Costs	13
16. Commencement, review and termination	13
17. Publication	13

Definitions

In this Memorandum of Understanding, unless the context requires otherwise:

"applicable law"	means any law (statutory, common or customary) applicable to Jersey to a matter covered by this MoU;
"Controller"	means the same as defined in Article 1 of the Data Protection (Jersey) Law 2018;
"Director of the JCSC"	means the individual appointed as Director of the JCSC;
"DPJL 2018"	means the Data Protection (Jersey) Law 2018 (as may be amended from time to time);
"DPAJL 2018"	means the Data Protection Authority (Jersey) Law 2018 (as may be amended from time to time);
"GDPR"	means the General Data Protection Regulation (EU) 2016/679;
"Information Commissioner"	means the Information Commissioner for Jersey (appointed pursuant to Article 5 of the Authority Law);
"Island"	means the Bailiwick of Jersey (" Jersey ")
"JCSC"	means the Jersey Cyber Security Centre;
"JDPA"	means the Jersey Data Protection Authority;
"JOIC"	means the Jersey Office of the Information Commissioner, which is the operating name of the JDPA;
"MoU"	means this memorandum of understanding;
"Parties"	means the JDPA/Information Commissioner and the JCSC;
"Person"	means a natural person, legal entity, partnership or unincorporated association;
"Processor"	means the same as defined in Article 1 of the DPJL 2018;
"Receiving party"	means either party receiving information from the other under this MoU;
"Sending party"	means either party when sending information to the other under this MoU.

Memorandum of Understanding ("MoU")

between the

**Jersey Data Protection
Authority ("JDPA")**

-and-

**Jersey Cyber Security
Centre ("JCSC")**

Recitals

- A. The JDPA is a statutory body established under the DPAJL 2018 to act as Jersey's independent regulator to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals. The JDPA consists of the Authority, the Information Commissioner and the staff of the office. The operational name for the Information Commissioner and staff of the office is the JOIC.
- B. The JDPA is empowered to take a range of regulatory action for breaches of the DPJL 2018, the DPAJL 2018 and by the Information Commissioner in respect of the Freedom of Information (Jersey) Law 2016 (the "**FOI Law**").
- C. Part 4 of the DPAJL 2018 places a broad range of statutory duties on the JDPA, including monitoring and enforcement of the DPJL 2018, promotion of good practice and adherence to the data protection obligations by those who process personal data. These duties sit alongside those relating to the enforcement regime under the FOI Law.
- D. The JDPA's (and Information Commissioner's) regulatory and enforcement powers include:
- a. conducting assessments of compliance with the DPJL 2018, the DPAJL 2018 and the FOI Law;
 - b. issuing information notices requiring individuals, controllers or processors to provide information in relation to an investigation;
 - c. issuing enforcement notices, warnings, reprimands, practice recommendations and other orders requiring specific actions by an individual or organisation to resolve breaches (including potential breaches) of data protection legislation and other information rights obligations;
 - d. administering fines by way of penalty notices in the circumstances set out in Article 26 of the DPAJL 2018;
 - e. issuing decision notices detailing the outcome of an investigation under the FOI Law;
 - f. certifying contempt of court should a public authority fail to comply with an information notice, decision notice or enforcement notices under the FOI Law;
 - g. investigating potential regulatory matters including liaising with the Jersey Financial Services Commission where appropriate; and
 - h. investigating potential criminal offences and liaising with the States of Jersey Police where appropriate.

- E. Article 15 of the DPAJL 2018 requires the JDPA, amongst other things, to:
- a. develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;
 - b. provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and the significant interests of data subjects;
 - c. engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data; and
 - d. promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.
- F. JCSC promotes and improves the Island's cyber resilience. JCSC is designed to act at arms length from Government of Jersey. JCSC supports critical national infrastructure, business communities, and citizens to prepare, defend and respond to cyber attacks in Jersey.
- G. JCSC supports Jersey in several ways:
- a. Acts as a Single Point of Contact for Jersey in relation to cyber security
 - b. Monitors information on global cyber threats that may pose a risk to the Island
 - c. Manages information security incidents
 - d. Discovers and manage vulnerabilities
 - e. Provides independent oversight of Jersey's overall cyber risk
 - f. Shares knowledge to increase Jersey's cyber resilience
 - g. Protects Jersey's cyber security reputation by ensuring that JCSC meets the appropriate best practice standards for cyber security
- H. The Government of Jersey is proposing a new Cyber Security (Jersey) Law. The law will provide clear foundations for JCSC's operations and introduce new requirements on Operators of Essential Service (OES).
- I. On 25 August 2023, by way of [Ministerial Decision](#), the Minister for Economic Development, Tourism, Sport and Culture made a Ministerial Decision delegating certain functions to the Director of the JCSC (formerly CERT.JE). The Director of the JCSC has the power to:
- a) Enter into agreements in respect of [JCSC] and relating to cyber security in Jersey including but limited to accepting tenders, placing and accepting orders, appointing consultants, agreeing and signing formal contracts and other forms of engagement;
 - b) consult and co-operate, as [JCSC] considers appropriate with relevant authorities and bodies.

- c) monitor and analyse all available information, whether or not provided directly to [JCSC], relating to internet and computer activity that may indicate a threat or risk which may affect Jersey, and take any action it considers necessary in response to those risks;
- d) analyse information received by it relating to incidents affecting Jersey, and take any action it considers necessary to mitigate, or assist in the mitigation of, the effect of those incidents;
- e) identify vulnerabilities in network and information systems which may affect Jersey, and take any action it considers necessary to resolve those vulnerabilities and risks arising from them;
- f) understand current global cyber threats and how these may affect Jersey, and take any action it considers necessary in response to those threats;
- g) raise awareness in Jersey of cyber security risks and threats, and responses and mitigations;
- h) provide, and co-ordinate the delivery of, cyber security services;
- i) enable and promote the sharing of cyber security information in Jersey;
- j) increase the level of cyber resilience in Jersey to reduce the risk, and impact, of incidents;
- k) represent Jersey's cyber security interests within Jersey and internationally, including by participating in international co-operation networks including the CSIRTs network; and
- l) provide support to enable effective cyber security in Jersey.

Purpose and Principles

1. The purpose of this MoU is to provide a framework for cooperation between the JDPA and JCSC. In particular, it sets out the broad principles of collaboration and establishes a framework for the exchange of relevant information to assist the JDPA and JCSC to carry out their respective functions. The MoU explains how the JDPA and JCSC will work together in the following areas:
 - a. The development of cyber security standards and guidance by each party
 - b. Assessing and influencing improvements in cyber security of regulated organisations
 - c. Information sharing
 - d. JCSC advising the JDPA on cyber security
 - e. JDPA advising the JCSC on data protection
 - f. Deconfliction between JCSC and the JDPA in relation to incident management
2. This MoU is a statement of intent that does not give rise to legally binding obligations on the part of either the JDPA or the JCSC. This MoU does not modify or supersede any laws or regulatory requirements in force in, or applying in, Jersey. This MoU does not affect any arrangements under other MoUs.
3. The Parties acknowledge that they may only provide information under this MoU if permitted or not prevented under applicable laws, regulations and/or requirements.
4. The Parties have determined that they do not exchange enough personal data to warrant entering into a separate data sharing agreement, but this will be kept under review.

Liaison

5. The Information Commissioner and Director of the JCSC shall, in the first instance, meet at least bi-annually at a time and date to be agreed.
6. The meetings will be an opportunity to discuss items of mutual interest and concern in relation to the interface and operation of the DPJL 2018 and any other matters as the Information Commissioner and Director of the JCSC shall deem appropriate.
7. The Information Commissioner and Director of the JCSC may be accompanied by members of their respective staff, and the meetings will be held in person unless agreed otherwise.
8. Nothing in this MoU will prevent more frequent meetings from taking place between the Information Commissioner and the Director of the JCSC and/ or their members of staff.

Scope of co-operation

9. The Parties acknowledge that it is in their common interest to collaborate in accordance with this MoU and enter into this MoU to *inter alia*:
- a. endeavour to assist in information and expertise exchange in order to develop effective cooperation, which may include organising joint professional educational and training programs, research, workshops, publications, study tours, qualifications and compliance activity; and
 - b. any other area of cooperation mutually agreed upon, in writing, by the JDPA and JCSC from time to time.
10. The JDPA and JCSC will seek to maintain a strong and constructive relationship. In particular the Parties will:
- a. seek to dispel confusions and misunderstandings about their different roles;
 - b. seek to achieve a complementary and consistent approach;
 - c. where possible, seek to assist one another with in-house training on their respective roles;
 - d. communicate regularly and meet at least bi-annually (or more often as appropriate) to discuss matters of mutual interest;
 - e. attend such meetings at appropriate levels of seniority, and equivalent levels of seniority (for example, Information Commissioner to Director of JCSC);
 - f. share, for comment, at an early-stage draft consultations or other documents intended for publication that might have significant implications for the other Party;
 - g. provide each other with a list of contacts to whom information exchanged under this MoU should be directed; and
 - h. keep under review the operation of this MoU and consult one another as appropriate on improving its operation and resolving any matters that may arise.
11. Information exchange will normally be responsive and will specifically relate to concerns as they arise. The Parties may also wish to proactively share emerging themes or trends.
12. This MoU does not impose on either the JDPA or JCSC any obligation to cooperate with each other or to share any information. Where a Party chooses to exercise its discretion to co-operate or to share information, it may limit or impose

conditions on that request. This includes where a) it is outside the scope of the MoU, or b) compliance with the request would breach the Parties' legal responsibilities.

Assessing and influencing improvements in cyber security

13. The JDPA considers that a key part of its work is understanding what cyber security standards have been achieved in the organisations within its remit, what changes are most urgently needed, and how these changes can be implemented.
14. Through its own guidance, the JDPA will encourage good practice and continuous improvement in cyber security amongst the organisations it regulates. For example, the Commissioner's guidance may promote the application of JCSC's technical standards and guidance, alongside other relevant good practice. The JDPA will continue to take into account how proactive an organisation is on cyber security matters and will recognise and encourage appropriate engagement with JCSC on cyber security matters, including the response to cyber incidents.
15. To support the JDPA's regulatory work, the JCSC may provide cyber security advice and assistance to the JDPA where requested. Any such decisions taken by the JDPA are the JDPA's responsibility.
16. The Cyber Security Policy Framework published by the Government of Jersey recognises the importance of working in partnership to successfully secure Jersey in cyberspace. Consistent with this, JCSC seeks to promote positive cyber security cultures, and to foster learning from experience and peers. The JDPA has regard to the value Jersey's Cyber Security Policy Framework places on partnership and collaboration when exercising the statutory functions in relation to cyber security.
17. The Parties will invite each other to participate collaboratively in awareness initiatives including Cyber Security Awareness Month. The Parties will, subject to resource constraints, support each other in such initiatives and will, where appropriate, encourage organisations to engage in relevant forums and working groups.
18. Where appropriate, the JDPA and JCSC will seek to amplify each other's messages and raise awareness of their respective roles; promote learning, consistent guidance and standards as well as key messages on data protection and cyber security.

Information sharing

19. The JDPA and JCSC may only provide information to the other if permitted, or not prevented, under applicable law. Subject to this, they will seek to share information that will enable or assist them to exercise their respective functions. This may include information relating to trends, application and interpretation of the applicable laws and joint initiatives and, in particular:
 - a. research projects;
 - b. promotional, education and training programmes and approaches;

- c. trends and techniques of enforcement efforts;
- d. audits, experience relating to inspections and privacy impact assessments;
- e. significant data protection and cyber security issues;
- f. notable law reform developments; and
- g. regulatory experience and developments.

20. The information sharing will not include details of specific complaints, individuals or businesses, or anything else for which disclosure would be prohibited by the applicable laws. For the avoidance of doubt, JCSC will not share information from an organisation it is engaged with due to a cyber incident with the JDPA unless it has the consent of the organisation to do so.

21. JCSC and the JDPA will share information to the extent permitted by law, and as appropriate and relevant to their respective missions, statutory functions and objectives. The detail of data sharing will be provided for outside this MoU and may include, but is not limited to:

- a. JCSC sharing relevant cyber threat information with the JDPA, including cyber threat assessments that are likely to affect OESs and other organisations regulated by the JDPA.
- b. The JDPA sharing information about cyber security incidents with JCSC (both on an anonymised, systemic and aggregated basis) to assist JCSC's role in helping to reduce harm from cyber security incidents in Jersey, and JCSC role as Jersey's Computer Security Incident Response Team (CSIRT), Single Point of Contact and National Technical Authority.

JCSC supporting the JOIC's own cyber security

22. JCSC may support the JOIC's own cyber security through the provision of technical tools and guidance, where requested. In some cases, JCSC may be able to provide advice to the JOIC, for example where significant changes are planned that may have implications for cyber security. The JOIC may receive JCSC support in the event it experiences a serious cyber security incident and where it requests such support.

JDPA supporting JCSC's own data protection

23. To the extent permitted by law, and cognisant of any conflicts with its regulatory role, the JDPA may support JCSC's own data protection through the provision of technical tools and guidance, where requested. In some cases, JDPA may be able to provide advice to JCSC, for example where significant changes are planned that may have implications for data protection.

Deconfliction between JCSC and the JDPA in relation to incident management

24. Where organisations report an incident to JCSC, and JCSC identifies that the case may be legally reportable to JDPA, the JCSC will remind organisations to be mindful of their regulatory obligations but will not opine on whether an

organisation may be under an obligation to notify nor make notifications to the JDPA on the organisation's behalf.

25. Where organisations have notified the JDPA of a cyber incident and it is identified through engagement with the affected organisation that the case may be a significant cyber incident which is relevant to the work of JCSC, the JDPA will recommend and encourage the organisation to notify JCSC.
26. When both Parties are engaged in managing a cyber security incident, subject to any legal constraints, the Parties will seek to co-ordinate their work to the extent reasonably practicable and appropriate, in order to minimise any disruption of the affected organisation's efforts to contain and mitigate any harm.
27. The JDPA's incident response phase will seek to make organisations aware of the need to prioritise engagement with JCSC and/or its cyber incident response providers in the immediate aftermath of an incident, in order to prioritise the mitigation of harm, identify the root cause of the incident, and take appropriate steps to prevent the incident reoccurring.
28. JCSC and the JDPA recognise that the priority for an organisation suffering an incident should be the incident's remediation and the mitigation of harm to the organisation, its customers, and Jersey and its residents more generally. Both Parties will seek to ensure that their interventions align with this priority and will provide each other with feedback where they view the other's approach to intervention may have worked against it.
29. The JDPA will recognise and incentivise appropriate engagement with JCSC on cyber security matters in its approach to regulation.
30. The JDPA acknowledges that where cross entity coordination in response to a cyber incident is required and justified by the potential impacts, JCSC will lead co-ordination in its role as national technical authority. Should the JDPA intend to issue public communications concerning an incident, it will share with JCSC (and other relevant law enforcement and sector regulators) such communications in advance.
31. All communications whether related to a specific incident or more generally will be mindful of the need to set out the distinct roles and responsibilities of the JDPA and JCSC.

No obligation to meet requests

32. This MoU is to be construed consistently with the right of either the JDPA or JCSC to decline or limit cooperation on particular matters, on the ground that to otherwise engage would be inconsistent with domestic laws, policies or priorities, or on the grounds of resource constraints or based on an absence of mutual interest.

Contact points

33. The JDPa and JCSC will designate a primary contact for the purposes of any communications under the MoU. Those individuals will maintain an open dialogue between each other in order to ensure that the MoU remains effective and fit for purpose. They will also seek to identify any difficulties in the working relationship and proactively work to minimise same.

Confidentiality

34. The Parties shall implement appropriate security measures to protect information transfers in accordance with the sensitivity of the information and any classification that is applied by the sending Party.

35. All non-public information shared under this MoU will be marked as such by the sending Party and marked with an appropriate security classification. For example, where information being shared by JCSC is classified as secret or above or is particularly sensitive or is otherwise marked for limited distribution (e.g. by use of the traffic light protocol or otherwise), JCSC and the JDPa will agree safeguards are put in place and maintained. This may include limiting distribution to named individuals within the JOIC.

36. Where one Party has received information from the other, it will consult (where permissible) with the other Party before passing the information to a third party or using the information in an enforcement proceeding or court case and notify the sending Party if it anticipates a legally enforceable demand for disclosure of the information.

37. Similarly, the receiving Party will notify the sending Party if any legally enforceable demand for disclosure of the information is received, unless this is not practicable because of urgency or prohibited by law;

38. If requested by the sending party in relation to a legally enforceable demand for disclosure of the information, assert any legal exemptions or privileges against disclosure on behalf of the sending party; and

39. If it is not practicable to notify the sending party of the receipt of a legally enforceable demand for disclosure of the information, assume the sending party will wish to assert any legal exemptions or privileges against disclosure.

40. Where confidential material obtained from, or shared by, the sending party is wrongfully disclosed by the receiving party holding the information, this party will bring this to the attention of the sending party immediately. This is in addition to obligations to report a personal data breach under the DPJL 2018 where personal data is contained in the information disclosed.

41. In accordance with relevant legislation, the JDPa and JCSC will protect the confidentiality and sensitivity of all unpublished and other confidential information received from the other, and maintain effective controls designed to minimise the risk of inappropriate disclosures.

42. The JDPA and JCSC will liaise where relevant, to the extent permitted by law and having regard to their respective objectives, on responding to enquiries from the public, including freedom of information requests and will consult each other before releasing information originally belonging to the other.

Retention and disposal of information

43. The JDPA and JCSC acknowledge that any information provided under this MoU must not be retained for longer than is reasonably required to fulfil the purpose for which it was sought or for longer than permitted under the DPJL 2018 or any other regulations of requirements. As soon as practicable after any information supplied under this MoU is no longer required, the relevant party will dispose of it in a secure manner.

Costs

44. Unless otherwise agreed between the Parties, each Party shall bear its own costs and expenses relating to matters described in this MoU, including without limitation the fees and expenses of their respective advisers.

Commencement, review and termination

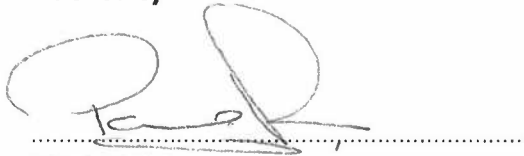
45. This MoU will take effect once both Parties have signed it.
46. The MoU will continue to have effect until terminated by either Party giving 30 day's advance written notice to the other Party.
47. In the event of the termination of this MoU, information shared under this MoU will remain subject to clauses 33-42.
48. The Parties will keep the operation of this MoU under review and will consult where necessary with a view to improving its operation and resolving any matters.
49. The Parties will consult in matters relating to any difficulties that may arise in relation to specific request made pursuant to or relating to any matters covered by this MoU
50. Any changes to this MoU can only be made by mutual agreement.

Publication

51. Either, or both, of the Parties may make a copy of this MoU or the text of it, publicly available.
52. The Parties agree that they will collaborate to agree upon language that each Party may use to publicise their relationship on each Party's website or in other media and agree not to publicise their relationship without the other Party's prior written consent.
53. Other than as specifically agreed upon in writing or as otherwise permitted by this MoU, each Party agrees not to use the name, trade name, trademark, or any

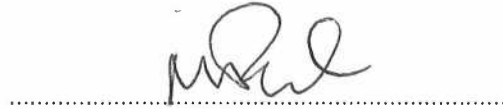
other designation of the other Party for any promotional purpose without the other Party's prior written consent.

**For the Jersey Data Protection
Authority**



Paul Vane
Information Commissioner
2 November 2025

**For Jersey Cyber Security Centre,
the Government of Jersey**



Matt Palmer
Director
2 November 2025