

Domestic and Family Violence Protection and Other Legislation Amendment Bill 2026

Submission No:	025
Submission By:	Office of the Information Commissioner
Submission Publication:	Making the submission and your name public

2 October 2026

Mr Nigel Hutton
Chair
Education, Arts and Communities Committee
Queensland Parliament

By email: eacc@parliament.qld.gov.au

Dear Chair,

Inquiry into the Domestic and Family Violence Protection and Other Legislation Amendment Bill 2026

The Office of the Information Commissioner (**OIC**) welcomes the opportunity to make a submission to the Education, Arts and Communities Committee's inquiry into the *Domestic and Family Violence Protection and Other Legislation Amendment Bill 2026* (**Bill**).

OIC's key considerations in relation to the Bill outlined below are aimed at strengthening privacy protections in the handling of monitoring information, particularly when it is not related to the electronic monitoring pilot (**EM pilot**).

About OIC

OIC is an independent statutory body that reports to the Queensland Parliament. The Information Commissioner is an Officer of Parliament and is charged with functions under the [Information Privacy Act 2009](#) (**IP Act**) and the [Right to Information Act 2009](#) (**RTI Act**).

The IP Act provides safeguards for the handling of personal information in the public sector environment. It sets out the Queensland Privacy Principles (**QPPs**) which govern the collection, management, use and disclosure of personal information by Queensland public sector agencies. The IP Act is intended to operate subject to the provisions of other Acts regulating personal information.

The RTI Act promotes openness, accountability and transparency by facilitating greater access to government-held information. It supports the administrative release of government-held information as a matter of course. Formal applications for government-held information under the RTI Act should be made as a last resort only.

Electronic monitoring pilot

The *Domestic and Family Violence Protection and Other Legislation Amendment Act 2025* amended the *Domestic and Family Violence Protection Act 2012* (**DFVP Act**) to support an EM pilot for high-risk domestic and family violence (**DFV**) perpetrators by enabling

prescribed courts to impose a monitoring device condition (**MDC**) on a respondent in certain circumstances when making or varying a domestic violence order (**DVO**). The *Domestic and Family Violence Protection and Other Legislation Amendment Regulation 2025* amended the *Domestic and Family Violence Protection Regulation 2023* (**DFVP Regulation**) to support the operationalisation of the EM pilot.

The stated purpose of establishing the EM pilot is to deter respondents from breaching DVO conditions related to the respondent's proximity to the aggrieved, named persons or particular locations.¹ The EM pilot commenced on 1 October 2025, operating from prescribed Magistrates Courts in Caboolture and Townsville.²

The Bill amends the DFVP Act and DFVP Regulation including to expand the EM pilot state-wide,³ mandate that all courts must consider making an MDC when making or varying a DVO, and enable police to access electronic monitoring information for domestic and family violence and other law enforcement purposes.

Information privacy

Personal and sensitive information

The IP Act defines 'personal information' as information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion, regardless of whether the information or opinion is true, or the information or opinion is recorded in a material form.⁴

'Sensitive information' is a subset of 'personal information' and attracts a higher level of protection under the QPPs. It is defined in Schedule 5 of the IP Act and includes an individual's racial or ethnic origin, religious beliefs or affiliations, sexual orientation or practices, criminal record, membership of a political/professional/trade association or trade union, and health information.

Queensland Privacy Principles

Government agencies handling personal and sensitive information must comply with the QPPs set out in the IP Act (unless an exception applies). Non-government agencies engaged to provide services through a service arrangement (contracted service providers) are also bound by privacy principle requirements.⁵ Key QPPs include:

- (a) open and transparent management of personal information (QPP 1)
- (b) collection of personal and sensitive information (QPP 3)

¹ [Report No. 5, 58th Parliament – Domestic and Family Violence Protection and Other Legislation Amendment Bill 2025](#) at p20.

² Section 1B(a) and (b) of DVFP Regulation.

³ Clause 57 of Bill.

⁴ Section 12 of IP Act.

⁵ Section 35 of IP Act.

- (c) notification of the collection of personal information (QPP 5)
- (d) use and disclosure of personal and sensitive information (QPP 6)
- (e) ensuring the quality of personal information (QPP 10)
- (f) security of personal information (QPP 11).

The retention period for personal information should be given careful consideration and tailored for specific purposes, or as a general rule limited to a strict minimum. In many surveillance cases, personal information need only be retained for a short period. A report by the Australian Human Rights Commission found that in 80% of cases, telecommunications data requested by law enforcement agencies was less than three months old.⁶ The potential risk of interfering with an individual's personal privacy can be significantly reduced by securely destroying the personal information as soon as it is no longer necessary for a specified purpose.

Key considerations

'Monitoring information' is defined in section 1F of the DFVP Regulation as 'information relating to a monitoring device or safety device, including information relating to alerts and notifications from the device or a person's geographical location.'

The Statement of Compatibility for the Bill provides that, 'Information collected from a monitoring device is deeply personal and can include data related to a person's daily movements and habits which can be used to build a picture of a person's religious, political, sexual, and other personal affiliations and associations.'⁷

OIC recommends that, as monitoring information comprises both personal and sensitive information, it should be handled by agencies in compliance with the QPPs, with careful consideration given to the retention period.

Court may impose other conditions

Current provisions

Section 57(1) of the DFVP Act provides that a court making or varying a DVO must consider whether imposing any other condition is necessary or desirable to protect the aggrieved or a named person from domestic violence. The principle of paramount importance to the court must be the principle that the safety, protection and wellbeing of people who fear or experience domestic violence, including children, are paramount (section 57(3)).

Section 66B(1) of the DFVP Act provides that, without limiting section 57, a prescribed court may impose an MDC on a respondent where certain criteria are met. The court must give reasons for imposing an MDC (section 66B(3)).

⁶ [Review of the mandatory data retention regime](#): Australian Human Rights Commission submission to the Parliamentary Joint Committee on Intelligence and Security (July 2019) at page 10.

⁷ Page 41.

Proposed amendments

Clause 8 inserts a new section 66BA into the DFVP Act which provides that a court must consider if it could impose an MDC under section 66B on the respondent. The court must provide reasons if it decides not to impose the MDC condition (section 66BA(3)).

As stated in the Explanatory Notes, mandating this consideration is intended to encourage courts to make full use of MDCs, while preserving judicial discretion to impose conditions that are necessary or desirable to protect the aggrieved in the particular circumstances.⁸

Key considerations

By mandating this consideration, OIC submits the volume of monitoring information being collected and handled by government agencies will increase substantially. As discussed above,, OIC submits that it should be handled in compliance with the QPPs, including relevant retention periods to reduce the risk of its misuse or unauthorised access.

Sharing information

Current provisions

DFVP Act

Section 66F(1) of the DVFP Act provides that a regulation may prescribe: how information relating to a monitoring device or safety device, including information relating to alerts and notifications from the device or a person's geographical location may be shared and with whom; the purpose for which the information may be shared; the entity responsible for recording or storing the information; and how the information will be recorded or stored.

Section 66F(2) of the DFVP Act provides that a person who obtains information relating to a monitoring device or safety device, including information relating to alerts and notifications from the device or a person's geographical location, must not use the information for a purpose other than the purpose for which the information was obtained or a purpose that is authorised or permitted under an Act. The maximum penalty is 100 penalty units or 2 years imprisonment.

DFVP Regulation

Section 1G(1) of the DFVP Regulation provides that monitoring information in relation to an MDC imposed on a respondent may be shared for the following purposes:

- (a) performing a function necessary for the imposition of the MDC
- (b) assisting the respondent to comply with the MDC

⁸ Page 22.

- (c) supporting or assisting the aggrieved or named person, including assisting the aggrieved or named person to use a safety device
- (d) assessing whether there is a serious threat to the life, health or safety of the aggrieved or named person because of domestic violence;
- (e) responding to serious threats to the life, health or safety of the aggrieved or named person because of domestic violence.⁹

Monitoring information may also be shared with the chief executive for the purpose of evaluating whether imposing MDCs on respondents has been effective in improving the safety, protection and wellbeing of people who fear or experience domestic violence (section 1G(2) of the DFVP Regulation).

Proposed amendments

Clause 60 inserts a new section 1KA into the DFVP Regulation which relates to sharing monitoring information at the request of the police commissioner. Section 1KA(1) provides that the police commissioner may ask a prescribed entity¹⁰ to give the commissioner monitoring information (other than information relating to a safety device), if the commissioner reasonably suspects the information would assist a police officer with—

- (a) assessing whether there is a serious threat to the aggrieved or a named person's life, health or safety because of domestic violence; or
- (b) lessening or preventing a serious threat to the aggrieved or a named person's life, health or safety because of domestic violence; or
- (c) performing a function for any other law enforcement purpose under the Act or another law.

The prescribed entity must give the police commissioner the information requested unless the entity does not possess or have access to the information (1KA(2)).

Clause 59 inserts the following subsection into 1G(1) to reflect this new purpose:

- (f) for monitoring information to be shared by a prescribed entity at the request of the police commissioner – assisting a police officer to perform a function related to a purpose mentioned in paragraphs (a) to (e) or another function for a law enforcement purpose under the Act or another law.

Key considerations

OIC recognises the paramount importance of the safety of DFV victim-survivors, and notes that section 29 of the IP Act exempts a law enforcement agency from complying with certain privacy obligations under that Act if the agency is satisfied on reasonable grounds that non-compliance is strictly necessary to undertake its functions to prevent,

⁹ Section 1G of DFVP Regulation.

¹⁰ A prescribed entity is defined in section 66A of DFVP Act.

detect, investigate, or prosecute a criminal offence or breach of a law imposing a pecuniary penalty.

The Bill confers a broad power on the police commissioner to request monitoring information from the holder of the information (currently Queensland Corrective Services) where the police commissioner 'reasonably suspects' the information will assist a police officer with performing a function for a law enforcement purpose under the DFVP Act or another law.

This means monitoring information will be able to be accessed and used by Queensland Police Service (**QPS**) for broader law enforcement purposes not connected to the EM pilot.

OIC submits consideration be given to strengthening privacy safeguards around accessing monitoring information for a purpose not connected to the EM pilot consistent with the IP Act, including:

- (a) replacing 'reasonably suspects' with the higher threshold of 'satisfied on reasonable grounds' consistent with the exemption in section 29 of the IP Act
- (b) narrowing the 'law enforcement purpose' to circumstances where access to the monitoring information it is strictly necessary to lessen or prevent a serious threat to the life, health or safety of an individual or to public health or safety.¹¹

Privacy and transparency by design

Privacy and transparency by design involve proactively embedding good privacy and information access practices into the design specification for all new or changed systems from the outset.

Undertaking a [Privacy impact assessment](#) (**PIA**) aligns with the privacy by design approach and involves identifying privacy impacts, assessing compliance with the QPPs, developing mitigating measures and formulating a privacy risk management plan.¹² It is recommended that PIAs are published where appropriate.

A transparency by design approach involves proactively considering and addressing how relevant privacy and right to information obligations will be met.

Key considerations

OIC recommends that a privacy and transparency by design approach is adopted by government agencies handling the monitoring information and submits that:

¹¹ This aligns with wording in schedule 4, part 1 (Permitted general situations) of the IP Act.

¹² Where sensitive information is collected, it is considered a reasonable step to conduct a formal, structured and documented risk assessment. See [Bunnings Group Limited and Privacy Commissioner \(Guidance and Appeals Panel\) \[2026\] ARTA 130 \(4 February 2026\)](#) at para 226.

- (a) public oversight of access to monitoring information would ensure greater accountability through the holder of the information reporting on the number of requests made for monitoring information not connected to the EM pilot
- (b) a PIA be undertaken prior to the implementation of any changes.

Thank you for the opportunity to make a submission. We trust our comments will assist the Committee in its work in reviewing the Bill. Should you require further information, please contact us at policy@oic.qld.gov.au or on 07 3234 7373.

Yours sincerely

A handwritten signature in black ink, consisting of a large, stylized capital 'J' followed by a series of loops and a long horizontal stroke.

Joanne Kummrow
Information Commissioner