NATIONAL OFFICE
Level 1, 16-20 Good Street, Granville NSW 2142
T: 02 8005 3333 **E:** members@nat.awu.net.au **W:** www.awu.net.au
Daniel Walton National and NSW Secretary

QUESTION FROM THE COMMITTEE

Is there any jurisdiction that has better workplace surveillance laws than New South Wales that we can look to?

GENERAL DATA PROTECTION REGULATION

The European Union has better workplace surveillance laws than New South Wales. In this paper we have provided a brief outline of the *General Data Protection Regulation* (GDPR), which came into effect on 25 May 2018 as the primary law regulating the use, recording, collection, processing, and storage of people's data, including workplace data. The GDPR has harmonised data protection laws across the Europe and replaced existing national data protection laws.

Article 3 – Jurisdiction

1) Businesses who operate:

   a) with an establishment in the EU, or

   b) outside the EU, that offer goods or services to individuals in the EU or monitor the behaviour of individuals in the EU.[1]

Who does this apply to?

2) Data processing performed on personal data by businesses, regardless of the size of the business.

Article 4 (1) and 4(2) – Key definitions:

3) Data processing is any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[2]

4) Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[3]

[1] Article 3.
[2] Article 4(2).
[3] Article 4(1).

What does it apply to?

5) Any information relating to an identified or identifiable natural person.[4]

REQUIREMENTS OF THE GDPR

6) The GDPR contains 11 chapters and 91 articles. The following paragraphs identify the parts of the GDPR that have the greatest impact on workplace surveillance.

Articles 4(2), 4(7) and 6 – Consultation and consent of workers

7) Personal data can be processed[5] only after consent has been obtained from the person whose data are to be processed for one or more specific purposes.[6]

8) The consent must be:
   a) freely given;
   b) specific;
   c) informed; and
   d) an unambiguous indication of the individual's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing.[7]

Article 6(1)(a) – Purpose

9) The controller can only process data for clear, specified, and legitimate purposes.

10) Further consent needs to be sought, where the purpose of the processing activities changes.[8]

Individual worker rights

11) Under the GDPR, individual workers have specific rights, such as the right to:

Article 4(7) – Right to erase data

a. request the controller i.e., their employer/business to delete their data in certain circumstances, including, but not limited to where the data is no longer necessary for the purpose for which it was processed, or where the individual withdraws their consent and there is no other legal ground for processing their data.[9]

Article 20 – Right to data portability

b. request transmission of data electronically to another organisation.[10]

[4] Article 4(1).
[5] Article 4(2).
[6] Article 6.
[7] Article 4(11).
[8] Article 6(1)(a).
[9] Article 4(7).
[10] Article 20.

Article 21 – Right to object

c. object at any time to the processing of an one's personal data. If an objection is made, the business must stop the data processing.[11]

Article 7(3) – Right to withdrawal of consent

d. withdraw his or her consent at any time. The withdrawal of consent will not affect the lawfulness of processing based on consent before the withdrawal.[12]

Articles 28(1), 32 and 5(1) – Handling of the data

12) A key requirement of the GDPR is that businesses must engage a data processor[13] to implement appropriate technical and organisational measures that ensure compliance with the GDPR and protect the rights and privacy of workers.[14]

13) The data must also be processed lawfully, fairly and in a transparent manner.[15]

Articles 50 to 78 – Regulator

14) Furthermore, the Regulation also obliges each European Member State to establish an independent supervising authority. The Regulation lists a vast number of functions and powers that an independent supervising authority must have, including but not limited to, monitoring compliance and enforcement of the Regulation, conducting investigations into breaches of the Regulation, issuing warnings to businesses, obtaining access to business premises and data, and advising on the application of the Regulation.[16]

Article 83(5) – Sanctions

15) The GDPR further gives independent supervisory authorities the power to impose administrative fines of up to €20 million or 4 per cent of annual worldwide turnover, (whichever is higher) for contraventions by businesses and their data processors.[17]

[11] Article 21.
[12] Article 7(3).
[13] Article 28(1).
[14] Article 32.
[15] Article 5(1).
[16] Articles 50 to 78.
[17] Article 83(5).