QUARTERLY UPDATE : Australia : June 2019

iGLOBAL LAW
GLOBAL LABOUR LAW

Overview	Legal Change	Action required
Whistleblowing New rules come into effect on **July 1st 2019** that significantly extend protection to 'eligible whistleblowers'.	The new rules : > expand the definition of 'whistleblower' to officers, employees, suppliers, regulated individuals and the relatives/dependents of the above; > allow and protect anonymous whistleblowing; > remove the whistleblower requirement of 'good faith'; > provide whistleblowers with immunity for liability for protected disclosures; > introduce civil penalties for victimising a whistleblower. The following are required to have a whistleblowing policy: public companies, large proprietary companies (having two of either: more than 49 employees; group revenue of more than A$25M; or group gross assets of more than A$12.50M) and corporate trustees of registrable superannuation entities. Policies must be in place by **January 1st 2020**. Penalties for breach have been significantly increased. The policy must: set out the protections; state to whom disclosures must be made, include information on how the company will support and protect whistleblowers and on how it will ensure fair treatment of someone mentioned in the protected disclosure; contain information on publicity for the policy and state how disclosures will be investigated.	Check if these rules apply to your company and if so make sure you have a compliant whistleblowing policy in place by **January 1st 2020**. Make sure you have an internal management structure that supports the whistleblowing scheme.
Directors Liability Personal liability of directors for salary underpayments.	In a recent case, 2 company directors who were 'wilfully blind' to the fact that employees were not being paid their due entitlements were held personally liable for the underpayments. This was despite the directors doing 'everything humanly possible' to ensure the payments were made. The liability was A$1.1million.	Company directors are responsible for ensuring company employees receive their entitlements. They should take this obligation very seriously. Wilful blindness is no defence.
Control of Biometric Data An employee who refused to use a sign-in fingerprint scanner was unfairly dismissed.	A court has held that an employee who refused to register his fingerprints for use when signing in and out of work and was then dismissed as a result, was unfairly dismissed. The chief reason given was that the employer's instruction to register his fingerprints was unlawful because the employer: (a) did not have a privacy policy; (b) had not issued a privacy collection notice; and (c) had not informed employees of the third parties who would have access to the data, all of which were in breach of privacy rules. In addition, given the threat of dismissal, employee consent to the data collection would not have been valid in any event.	Whether or not you collect biometric data, the case demonstrates the need to ensure your workplace data privacy policies and practices comply with the law.

This is a high level general update only. Legal advice should be obtained on specific circumstances.

www.igloballaw.com
joanne.martin@igloballaw.com