

## Ireland – Data Privacy

The Constitution of Ireland does not provide an express right to privacy, however, it has been held to establish an implied right to privacy. The Data Protection Act 1988 (the “Act”) implemented the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Ireland, as a member of the European Union (“EU”), was required to implement the EU Data Protection Directive 95/46/EC (the “Directive”) into its national legislation. The Directive was implemented in Ireland pursuant to the Data Protection (Amendment) Act 2003, which amended the Act. The Office of the Data Protection Commissioner (“DPC”) enforces the Act.

Entities that “process” personal data, as defined, but do not exercise control over the contents and use of that data, are “data processors”. A data processor is distinct from the data controller for whom they are processing the personal data. A “data controller” is the individual or legal person who controls and is responsible for the keeping and use of personal information on a computer or in structured manual files.

| Collection and Processing of Personal Data |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Compliance Alternatives</i>             | <p>Personal data may be processed in circumstances including where it has been fairly obtained and: 1) the employee has given consent; 2) processing is necessary (a) to perform a contract to which the employee is a party (N.B. an employment relationship is a de facto contract) or (b) to take steps at the employee’s request prior to entering into a contract; 3) processing is necessary for compliance with a legal obligation; 4) processing is necessary to protect the vital interests of the employee in certain circumstances; 5) processing is necessary for certain public purposes; or 6) processing is necessary for the legitimate interests of the employer, except where the processing is unwarranted by reason of prejudice to the fundamental rights and freedoms or the legitimate interests of the employee.</p> <p>Data shall not be further processed in a manner incompatible with the purpose, data shall be relevant and not excessive and data should not be kept for any longer than necessary for these purposes. An employee should know the name of the data controller, the purpose of collecting data, the persons or category of persons to whom data may be disclosed and should be aware of their right to access and rectify data.</p> <p>Sensitive data (e.g., data relating to racial or ethnic origin, political opinions, party affiliation, religion, physical or mental health, sexual life, criminality and trade union membership) may be processed only if the conditions for personal data processing (set out above) are met, along with an additional condition including 1) employee’s explicit consent to the processing, 2) processing is necessary for a right or obligation conferred or imposed by law on a data controller in connection with employment, or 3) processing is necessary for certain public purposes.</p> <p>Data processors have a very limited set of responsibilities under the DPA in comparison to data controllers. Data processors are essentially required to: (i) register their activities with the DPC if required (see below); (ii) act only on and in accordance with the instructions of the data controller; and (iii) keep personal data secure from unauthorised access, alteration, disclosure, destruction or any other unlawful processing. A data controller should enter into an appropriate processing agreement with a data processor.</p> |
| <i>Disclosure/ Registration</i>            | <p>2007 Regulations (S.I. 657 of 2007) require that all data controllers and data processors register with the DCP unless they come within a list of exemptions or are specified as not obliged to register by Ministerial regulations. The exemptions from registration are very broad. The main categories of data controller required to register with the Data Protection Commissioner (if they hold personal data on computer) are: Government Bodies/Public Authorities, banks and financial/credit institutions, insurance undertakings (not including brokers), data controllers whose business consists wholly or mainly in direct marketing, data controllers whose business consists wholly or mainly in providing credit references, data controllers whose business consists wholly or mainly in collecting debts, internet access providers, telecommunications network or service providers, health professionals processing personal data related to mental or physical health, data controllers processing genetic data, data controllers whose business consists of processing personal data for the supply to others, other than journalistic, literary or artistic purposes. Any data processor processing on behalf of a data controller in one of these categories must also register.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <i>Other Requirements</i>                  | <p>An employer must keep employees’ personal data secure from unauthorized access, disclosure, destruction or accidental loss. The nature of security used may take into account what is available technologically, costs and sensitivity of data.</p> <p>An employer must ensure that employees’ personal data is kept accurate and up-to-date.</p> <p>A copy of the personal data must be given to the individual on their request and they must be permitted to correct errors.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

This summary is intended to reflect local law and practice as at 1 May 2013. Please note, however, that recent amendments and legal interpretations of the local law may not be included in these summaries. In addition, corporate governance, administration, and option plan design facts that are specific to your company may impact how the local laws affect the company’s equity based compensation plans. With these matters in mind, companies should not rely on the information provided in this summary when implementing their stock plans.

## Transfer of Personal Data

### *Compliance Alternatives*

Cross-border transfer of personal data to a country outside the European Economic Area ("EEA") is permitted if that country ensures an adequate level of data protection, as determined by the EU Commission or the DPC (as per list of EU approved countries)

Cross-border transfer of personal data to a country outside the EEA with inadequate data protection is permitted if the transfer is: 1) consented to by the employee, 2) required or authorized under an enactment, convention or other instrument, 3) necessary for the performance of contract to which an employee is a party, 4) necessary for the taking of steps at the request of the employee with a view to his or her entering into a contract with the employer, 5) necessary for the conclusion of a contract between the employer and a third party, that is entered into at the request of the employee and is in the interests of the employee, or for the performance of such a contract, 6) necessary for the purpose of obtaining legal advice, 7) necessary to urgently prevent injury or damage to the health or property of an employee in certain circumstances, 8) part of the personal data held on a public register, 9) necessary for reasons of substantial public interest or 10) authorized by the DPC where the employer adduces adequate safeguards with respect to the privacy and fundamental rights and freedoms of individuals and for the exercise by individuals of their relevant rights under the Act or the transfer is made on terms of a kind approved by the DPC as ensuring such safeguards (e.g., standard or model contractual clauses, US/EU Safe Harbor principles or 'binding corporate rules' for multi-national companies).

The DPC states that a best practice approach would be for a data controller planning an international data transfer to consider first whether the third country provides an adequate level of protection and to satisfy himself or herself that the exported data will be safeguarded in that country. In the case of data transfers to the US, the controller exporter may want to encourage the importer to subscribe to the Safe Harbor principles. If the level of protection in the third country is not adequate in the light of all the circumstances surrounding a data transfer, the data controller should consider providing adequate safeguards through use of EU-approved 'model contracts' or 'binding corporate rules'. Only if this is truly not practical and/or feasible should the data controller consider relying on data subject consent or the other derogations provided for in law. This is particularly so in the case of repeated transfers of personal data, especially where the data involved is sensitive or where there could be any question over whether there is a fully free consent. It is not generally recommended to rely on consent alone as a basis for transfers outside of the EEA in an employment context.

Where employees' personal data is transferred within a multinational group within the EEA, explicit employee consent is not necessary. However the employee should be aware that data is being transferred to a different company. If this data is sensitive, explicit consent would be necessary.

The commissioner has the power to prohibit the transfers of personal data to any country, except in cases where the transfer is required or authorized by law, or where the transfer is required by an international agreement which Ireland is obliged to enforce.

### *Other Requirements*

In summary, the basic Rules of Data Protection are as follows.

A data controller must:-

- 1) Obtain and process information fairly.
- 2) Keep it only for one or more specified, explicit and lawful purposes.
- 3) Use and disclose it only in ways compatible with these purposes.
- 4) Keep it safe and secure.
- 5) Keep it accurate, complete and up-to-date.
- 6) Ensure that it is adequate, relevant and not excessive.
- 7) Retain it for no longer than is necessary for the purpose or purposes.
- 8) Give a copy of his/her personal data to an individual, on request.

Specific advice may be required regarding any of the general principles set out above.

This summary is intended to reflect local law and practice as at 1 May 2013. Please note, however, that recent amendments and legal interpretations of the local law may not be included in these summaries. In addition, corporate governance, administration, and option plan design facts that are specific to your company may impact how the local laws affect the company's equity based compensation plans.

With these matters in mind, companies should not rely on the information provided in this summary when implementing their stock plans.