Data privacy guidelines for using Wellnomics Risk Management

Wellnomics® White Paper

Wellnomics Limited

www.wellnomics.com

Ref 062015

1.1-01062015

Contents

Data Privacy Requirements

Being seen to protect the privacy of employees is increasingly important and many organizations have policies regarding privacy of employee data. In some countries there is special legislation specifically outlining legal requirements for data privacy (see later section *Data Privacy Legislation*). In general, these data privacy requirements can be summarized with the common principles below:

1. Data about employees (referred to as "personal data") should only be collected if there is a specific purpose for its collection. You can't just collect data because it "might be useful one day".
2. The amount of data collected should be limited to just that needed to fulfill the identified purpose.
3. Data should not generally be used for other purposes than that for which it was collected[†].
4. Employees should be informed about the data collection and the purpose for which it is being collected.
5. Employees have the right to request access to the data stored about them.
6. Data should not be kept longer than is necessary.
7. Data should not be transferred to a foreign country unless it can be assured that the data will be only used in accordance with the privacy requirements of the originating country.

Furthermore, when accessing and using this data:

1. Access to the data should only be provided to those who have a legitimate need to use the data (in accordance with the original purpose of its collection).
2. When someone is given access to data, they should only be given access to the minimum data required for them to complete their assigned tasks.
3. Access to sensitive personal data[‡], such as health information, should only be provided to people qualified (or trained) to understand and interpret this information correctly.

It should be noted that data privacy requirements only apply to "personal data", this being data that relates to an individual who can be identified from it. Group statistics where specific individuals cannot be identified, such as averages or distributions, are therefore not covered by data privacy legislation. This said, when using aggregate data it must be ensured that the group size used is large enough that information about individual members of the group cannot be inferred. For example, if high stress levels occur for 66% of the members of the group, and there are only 3 people in the group, then it is going to be easy to identify the employees that have this issue present.

[†] Although there are exceptions to this, such as using the data for aggregate purposes, or where the data is first anonymized. Furthermore, other uses can be considered if done in consultation with employees.

[‡] Sensitive data is a special distinction made in data privacy for personal data that may be seen as particularly sensitive, such as data on physical or mental health. There can be stricter requirements around handling of "sensitive" personal data.

Health and Safety legislation and employee consent

Employee consent may be required for collecting and using data, particularly sensitive data such as that about health. This could be seen as an issue when it comes to using Wellnomics Risk Management – with employee consent being required before the data on computer use, or assessments of discomfort, can be collected.

However, most data privacy legislation has specific exemptions for the collection of data for health and safety purposes. Employers have a legal responsibility to ensure the health and safety of their employees at work and most health and safety legislation specifically requires the collection of employee information as part of conducting risk assessments and in identifying early signs of injury (i.e. early reporting of discomfort). Data on exposure (time on computer, number of breaks), pain symptoms, workstation setup and posture, and even psychosocial factors, are all legitimate data for the purposes of conducting accurate risk assessment.

As an employer cannot fulfill his legal responsibilities without collecting this information employee consent is not required. In fact, health and safety legislation normally places a responsibility on employees to cooperate, as employees also have a duty of care to ensure their own health and safety at work. This includes co-operating with any employer initiatives aimed at achieving this (so long as these initiatives are reasonable of course).

This means that (i) the collection of data by Wellnomics Risk Management cannot contravene data privacy requirements, and (ii) no employee consent is required for the collection.

Of course, although health and safety obligations override data privacy limitations when it comes to the collection of data by Wellnomics Risk Management, they still apply to the use and access of this data once its collected. This means the data on individuals collected by Wellnomics Risk Management should only be used for the purposes of health and safety, and access to it should only be by those staff responsible for health and safety.

This does not preclude the use of the data for other purposes in an aggregate or anonymized form. However, it is recommended as good practice to inform staff if the data is to be used for any other purposes, even if this is done in an anonymous form.

How Wellnomics Risk Management supports data privacy

Wellnomics Risk Management supports full compliance with data privacy legislation and policies. It achieves this through the following:

1. Wellnomics Risk Management records the minimum data[§] on computer use required to calculate exposure risks. The product does not record any detailed data such as what words were typed, which documents were edited, or which websites were viewed. Nor does it record information on work patterns during the day. Instead, only *exposure* data relevant to determining WMSD related risk is recorded. Data such as total hours at the computer, number

[§] Note that Wellnomics Risk Management can record additional information, such as application usage, which is used by some organizations. But this data recording can be disabled by default and is not required in order to do risks analysis. For full information on what statistics WorkPace can record see Wellnomics white paper – *What statistics does Wellnomics WorkPace record on computer use?*

of breaks, and total keystrokes typed. This ensures the employees privacy with respect to their activity at their computer is preserved as much as possible.

2. Wellnomics Risk Management is designed to restrict access to raw data such as statistics on computer use, or answers to assessment questionnaires, which could be mis-interpreted or used for other non-health and safety purposes. The product instead focuses on providing interpreted data that is designed for the intended purpose of managing the health and safety risks of employees. This is done by converting computer statistics and questionnaire answers into "risk factors" that indicate the simple presence or absence of a particular known risk for RSI. For example, the risk factor "High computer use" does not report the actual number of hours of computer use, but simply whether the use was above or below a *risk threshold*.
3. Each employee can login to the system and has full access all data recorded about them, including historical data.
4. A Privacy and Access Control feature allows the level of data access to be controlled for different users (or "roles"). This is done in two ways:
    a. A **Data Privacy Level** controls whether someone can see **Individual** or just **Group** data. For example, a manager may be restricted to seeing just group data such as average risk levels or the top risk factors for their department. Only OH&S personnel may be allowed to view data on individual employees.
    b. A **Data Access Level** controls what level of data a user can see. For example, access to data on computer statistics may be restricted to just OH&S personnel who are able to interpret this data as part of conducting a detailed evaluation for an employee who is at high risk or has reported an injury.
5. If someone is only given access to Group data, then a minimum group size can be set (e.g. 50 users) to ensure that anonymity is maintained in any group reporting.
6. There are four "roles" defined in the product. Data access and privacy levels can be set separately for each role. Furthermore, each role is automatically restricted to only viewing data on the employees they are responsible for.

Role	Description
End user	An employee with no reporting staff. Can only see their own data.
Manager	Can only see data about their reporting staff (both direct reports, and employees further down the reporting hierarchy).
Local Administrator	Generally company OH&S personnel or ergonomists. Is only given access to users within the group or department they are responsible for.
Global Administrator	The company OH&S manager or a senior manager. The only role that can access data for all employees in the organization.

Data imported from the organization's HR database is used to define which staff have each role and which employees they are responsible for. Tools are provided to allow the Wellnomics Global Administrator to then adjust access for different users.

Guidelines for using Wellnomics Risk Management in accordance with data privacy requirements

Inform staff

Inform staff about the project making sure to cover:

- What data will be collected.
- How the data will be used.
- Who will have access to the data.

Because the use of Wellnomics Risk Management will likely be a new concept to staff it will be helpful to include some background on the project. For example, remind staff that as an employer you are responsible for the health and safety of employees at work. This means you have a legal responsibility to take steps to protect staff from the risks of RSI/WMSD. One of the steps required to achieve this is to perform risk assessments for each employee and measure their exposure to the risk factors that can cause RSI. The latest research now shows that time using the computer and the level of breaks are as important as workstation setup in determining risks. This means that monitoring information on exposure is now required as well in order to accurately assess risks.

Perhaps refer employees to some background information on RSI risks – causes and prevention, which explains the multi-factorial nature of RSI.

Identify roles for managers

Review your OH&S processes and determine what responsibilities your managers are expected to take on regarding the management of health and safety risks of their reporting staff. As access to personal data by their own manager is likely to be the most sensitive area for employees restricting access by managers to only the data needed to fulfil their responsibilities is important.

Depending upon managers responsibilities, some different options are outlined below:

OH&S responsibilities	Recommendation
None	The manager may have no specific OH&S responsibilities, other than to co-operate with OH&S staff when requested. Managers may still be interested to monitor the general risk levels of their staff or department. **Data Privacy Level** = Group **Data Access Level** = Overall Risk

Only responsible for ensuring staff complete OH&S training & assessment requirements	The manager may only be responsible for facilitating the OH&S process by ensuring their staff meet the OH&S requirements of completing the training and risk assessments, and their staff have WorkPace installed. **Manager Data Privacy Level** = Group **Manager Data Access Level** = Overall Risk
Responsible for monitoring risk levels and taking action to reduce risks, but on a group basis only	The manager may only be responsible for taking action at a group level – e.g. addressing risk factors that are common to their staff or department, and monitoring the overall risk levels amongst their staff to ensure they are being kept below targets. The manager may therefore only need to look at group information to identify if risks are high, and what the common risk factors are. They can then call on OH&S assistance to help address risks on an individual basis amongst their staff if risk levels are high. **Manager Data Privacy Level** = Group **Manager Data Access Level** = Risk Factors
Expected to identify high risk staff and ensure appropriate action is taken to reduce risks.	The manager may be expected to take an active role in managing the risks of their staff. Identifying which staff are high risk, and then working with those staff to address those risk factors in co-operation with OH&S support staff. **Manager Data Privacy Level** = Individual **Manager Data Access Level** = Risk Factors

It is not recommended that managers be given access to computer use statistics.

OH&S staff

OH&S staff should be setup as Local Administrators in Wellnomics Risk Management. Each OH&S staff member should then be given access to just the group or groups of staff they are responsible for. OH&S staff will normally be given full access to data on individual employees within their departments.

Local Administrator Data Privacy Level = Individual

OH&S staff will need access to at least the Risk Factors level of data.

Local Administrator Data Access Level = Risk Factors

This will allow them to view risk reports for employees and see the most detailed level of risk information.

Access to computer use statistics

Wellnomics Risk Management is able to provide basic reporting on computer use statistics, such as time using the computer, time using the mouse, number of days using the computer, and number of breaks taken, etc.

Generally speaking access to this data is not needed to manage the health and safety of employees. However, in some circumstances these statistics may be helpful in better understanding the work patterns of a high risk employee or an employee who has reported an injury (have they been working 7 days week? Have they been working overtime with days of over 8 hours at the computer?). These statistics can also be important in the case of a dispute or legal claim – providing objective evidence of the computer use exposure of the individual.

Depending upon your organizations policies you can decide to either provide OH&S staff with access to this data (**Local Administrator Data Access Level** = Statistics) or you can restrict this access only to the Wellnomics Global Administrator, who can then provide reports on this data on a case-by-case basis.

f OH&S staff are provided with access to computer use statistics it is important that they are trained to interpret this data and they do not provide copies of the data to other parties.

Sending data across international borders – the Safe Harbor Framework

Wellnomics Risk Management uses a single server on which data for all employees is stored. For an organization with employees in multiple countries this means personal employee data will be transferred across international borders. This is potentially an issue due to data privacy legislation commonly restricting the transfer of personal data to other countries that do not comply with the data privacy legislation of the originating country.

For example, the European privacy legislation effectively prohibits the transfer of personal data to non-European Union nations that do not meet the European "adequacy" standard for privacy protection. With the United States taking a quite different approach to privacy - a sectoral approach relying on a mix of legislation, regulation, and self regulation – there is a potential issue with storing data on European based employees on a server located and accessed in the United States.

In order to bridge these different privacy approaches and provide a streamlined means for US organizations to comply with the European Privacy Directive, the US Department of Commerce in consultation with the European Commission developed a "Safe Harbor" Framework[**].

Under the Safe Harbor Framework, US companies can “self-certify” to the US Department of Commerce that they have privacy policies that conform to the seven Safe Harbor principles: Notice, Choice, Transfer, Access, Security, Data Integrity and Enforcement. These seven principles largely seek to replicate the common data privacy principles outlined in the first section of this document.

Using Wellnomics Risk Management across multiple countries

If an organization will be using the Wellnomics Risk Management across different countries that are not covered by the same data privacy legislation, for example, US and UK, or US and Australia, there are several options:

1. Locate the Wellnomics Risk Management data server in the jurisdiction with the strictest data privacy requirements – for example, in Europe.

[**] http://www.export.gov/safeharbor/

2. If the server is located in the US, use the Safe Harbor Framework to self-certify data privacy compliance.

Note that if your organization already has significant cross-border data transfer between the US and Europe you may already have an existing Safe Harbor certification. For example, if employee human resources data is stored in a common database at a US based head office. The data collected by Wellnomics Risk Management may be already covered under this certification, or may be able to be covered through a modification or extension to the existing certification.

The Data Privacy Legislation

This document is based upon a review conducted by Wellnomics of the UK Data Protection Act (1998)[††] and the Australian Privacy Act (1988)[‡‡]. The UK Data Protection Act (1998) is based upon the European Directive 95/46/EC[§§] which covers all European Union members, and so gives a good proxy for data privacy requirements in other European countries. The Australian Privacy Act (1988) is based upon 10 Australian National Privacy Principles[***] which are similar to the principles outlined in the UK Data Protection Act. Overall the principles enshrined within these two acts, and their relation to health and safety legislation, are expected to be representative of data privacy legislation in other countries where such legislation exists, although Wellnomics has not undertaken any review of such legislation in other countries.

Disclaimer

This document represents Wellnomics interpretation of data privacy leglisation and does not constitute a legal opinion. Wellnomics Ltd cannot give any guarantees as to the accuracy of the information contained herein, or the interpretations or opinions expressed. Anyone reading this information or using the Wellnomics product is advised to take their own legal advice on meeting legislative privacy requirements.

[††] http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1
[‡‡] http://www.privacy.gov.au/law/act
[§§] http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf
[***] http://www.privacy.gov.au/materials/types/infosheets/view/6583