TEMPORARY COVID-19 PRIVACY NOTICE (Employees & Sub-contractors)

At Piranha Parcels Limited, we are committed to protecting your privacy. This policy applies when we are acting as a controller of personal data, i.e. where we have determined the purposes and means of the processing of that personal data. It applies to all staff.

➢ ***Throughout the Coronavirus covid-19 pandemic and during the supply of services it may be necessary for Piranha Parcels Limited (the controller) to obtain personal health data from you (the processor), in the event that you test positive for covid-19. Please read the guidance notes below;***

➢ ***This data may be shared with third parties such as, but not limited to, local authorities, customers, suppliers & work colleagues for the purposes of contact tracing, prevention of the spread of coronavirus Covid-19 & disease containment practices only. We will only share your personal data with other third parties to the extent that the disclosure is reasonably necessary for us to comply with health protection & wellbeing obligations in relation to your engagement with us or to comply with the law.***

We will process your personal data for the purposes of complying with your contract of engagement, maintaining reasonable records of work activities and the promotion and supply of our products and services. The legal basis for this processing is that it is necessary for the performance of your contract of employment/contract of engagement with Piranha Parcels Limited and Piranha Parcels Limited's compliance with legal obligations.

We will store your personal data only for as long as necessary to fulfil the purposes for which we collected it, including for the purposes of satisfying any legal, accounting or reporting requirements. Details of retention periods for different aspects of your personal data are available in our Control of Documented Information Procedure, available in section 8.0 Data Protection Management of our ISO9001 Quality Management System.

As you are providing us with your personal data, it is important to us that you are aware of the following rights that you have in relation to our processing of that personal data.

You can be provided with a copy of any personal data concerning you that we process, unless that would affect the rights and freedoms of others. You can also be provided with information on how that personal data is processed by us.

You can ask us to provide your personal data, either to yourself or to another data controller, in a structured, commonly used and machine-readable format.

You can have us rectify any personal data of yours that we hold that is inaccurate or incomplete. In certain circumstances, you can also ask us to erase or restrict the use of any of your personal data that we process.

You can exercise any of the rights listed above by contacting us using the details at the bottom of this notice. If you are unhappy with any aspect of how we processed your personal data or your request to exercise a right, you can lodge a complaint with the Information Commissioner's Office.

Piranha Parcels Limited is incorporated and registered in England and Wales with company number 12941429 and whose registered office is at 3 New Bridge Square, Swindon, Wiltshire, SN1 1HN. We are contactable by email at admin@piranhaparcels.com.

REQUIREMENT OF HEALTH DATA

Information about an individual's health is a 'special category' of personal data, and the ability to collect health data lawfully is more limited. The GDPR defines health data as any information related to an individual's physical or mental health. Therefore, health data not only covers information that is "obviously" health-related – such as a description of symptoms – but also more general information. This includes information on past or present health conditions, but also information concerning the person's future health. So, data that the company receives through self-declaration or questionnaires from employees or external parties to check their current health status is always sensitive data that requires protection.

LAWFULNESS OF PROCESSING

Health data is subject to the processing prohibition in accordance with Art. 9(1) GDPR, which results in stricter requirements in which processing is permitted. The legal basis for processing health data regarding protection of employees against coronavirus would be:

Art. 9(2)(a) GDPR permits data processing on the basis of consent of the employee or sub-contractor. It must be taken into account that a consent cannot be given by implication or an opt-out procedure. Consent for processing personal data must be given in an informed and voluntary manner and not per the general consent requirement of the national law. The most appropriate would be a written consent or an oral consent. Both have to be filed with the purpose of processing and date of consent for accountability reasons by the controller. The disadvantage is since the consent is voluntary it can be freely revoked at any time. A comprehensive use and evaluation would therefore not be guaranteed. In addition, the question of how to obtain the consent of all potentially affected persons who have had contact with a covid-19 positive patient is also an issue.

According to Art. 9(2)(i) GDPR, the processing of sensitive data is permissible due to the increasingly rapid spread of the coronavirus, if it concerns the area of public health, which includes in particular "serious cross-border threats to health". It should be considered that this is a flexibility clause that's why the national legislature may, under certain conditions, create its own regulations.

As a similar legal basis, the exceptional circumstances of Art. 9(2)(g) GDPR could apply. According to this, the national legislature can enact legislation that allows companies to process special categories of personal data if there is a substantial public interest. Such an interest certainly exists in the case of the fight against coronavirus, but it is precisely the national legislature, which must create appropriate specific provisions, which specify the processing and conditions of the required data in more detail.

PRIVACY MEASURES

Every processing of health data of employees concerning coronavirus must be necessary to fulfil the data minimisation principle. Companies as controllers should continuously reflect whether the sub-contractor or employees' health data is "adequate, relevant and limited to what is necessary in relation to the" coronavirus safety purpose. It should be considered how the same goals can be achieved by a reframing from a question or an alternative procedure.

The normal requirements around provision of information to be provided to the related data subjects will apply. Employees about whom health data is collected should receive a privacy notice, before or at the time of collection, that details the main characteristics of the data use. Companies can either update existing privacy notices or if they do not cover disease containment – create a new privacy notice dedicated to coronavirus. All data subject rights will remain relevant for companies and will need to have processes in place to deal with requests, especially exercising the right of access and right of erasure (Article 12-21 GDPR).

Given the nature of coronavirus-related data processing activities, when sensitive health data and evaluation of health risks is involved according to Article 35 GDPR a Data Protection Impact Assessment has to be undertaken by organisations. A Data-Processing-Agreement or Joint-Controller-Agreement should be put in place if sub-contractor or employees' health data is passing to another entity. The GDPR allows companies to outsource the collection and analysis of coronavirus-related personal data, until this outsourcing does not reduce the level of data protection. According to Article 30 GDPR a Record of Processing Activities should be maintained and updated in a timely and accurate manner to reflect the new personal health data processed.

Moreover, appropriate safeguards as technical and organisational measures have to be implemented and ensure the security of the personal data to the level of risk. It is recommended to store or process sub-contractor & employees' health data in an encrypted file on a hard drive. Only sub-contractors or employees from whom it is strictly necessary to undertake their tasks should have access to the sub-contractors or employees' health data. Lastly, the process of deletion has to be initiated by the company after the legal retention period or fulfilment of purpose has been lapsed.

Companies can collect and store health data relating to their sub-contractors or employees through self-disclosure or questionnaires on their recent locations and indications of potential symptoms and their indicators. They can also conduct surveys on specific occasions after business trips or contact with suspected persons. In the event of a positive finding on an employee by an official body or in the event of confirmed contact with a person who tested positive, it would be permissible to process information about the employee or sub-contractor concerned, e.g. time and close contact persons and measures taken. But it should not be permissible to require all staff to provide information on their travel destinations and health status or collect blanket information about flu symptoms from employees & sub-contractors or to have them communicated by colleagues.

The fever testing of personnel on company premises and other medical measures can be justified under strict conditions. A fever test can certainly be regarded as permissible if the results are only used for an admission control with the necessary and limited decision undertaken by a simple "yes or no", without further processing of information it would not constitute the processing of personal data.

In order to ensure that employees & sub-contractors can be warned at short notice and not when they appear at work, companies may also request and temporarily store the current private phone number of their staff with consent. At latest after the end of the pandemic, the collected contact private contact data must be deleted by the company.

Other measures currently under discussion should be viewed extremely critically, e.g. mobile phone tracking of infected persons in order to better identify contact persons or the naming of specific addresses of infected persons. In any case, this could only be carried out by the state, the governmental agencies authorised to protect public health.

SUMMARY

Knowing about persons' Covid-19 disease status can lead to a stigmatisation for the individual. Mentioning the name of the infected should therefore be avoided. Simultaneously, staff who have been in direct contact with an infected person must be warned and be excused from work themselves to reduce the risk of infection. Such a measure can be carried out on a department or team basis. If, in exceptional cases, this is not sufficient, the company must contact the health authorities and request their decision.

Companies should only collect necessary personal data. In the context of coronavirus containment, this means collecting the minimum information needed to evaluate the risk that an individual carries the virus and take proportionate risk-based measures. In terms of data collection method, the least intrusive and disturbing option should be selected. This may require adopting a gradual risk-based approach, such as providing questionnaires with targeted 'yes or no' questions to carry out a first screening of individuals' coronavirus threat and review the questionnaires to ensure only required and necessary information is collected.

As long as no official written order has been issued, companies are only free to collect and store the names and contact details of their employees & sub-contractors on the basis of consent for the purpose of transmitting them to the health authorities on request. In this case, the duration of storage should be based on the presumed incubation and detection period of infections.

In view of the infection rate on the one hand, and the intensity of an intrusion into the privacy of employees when accessing health data on the other, a collection and evaluation can be regarded as proportionate. Still the potential for abuse from the collected health data is great, it would be relatively easy to draw further conclusions about religious beliefs or sexual orientation. However, the risk to public health is increasing and is existential. It is then up to find a good balance between data and health protection of the employees.