To: [INSERT DETAILS]

Date: [INSERT DATE]

**Re: Policy with regard to Disclosure of Vaccination Status in order to access Premises / Goods or Services**

Dear Sirs,

I refer to the above referenced matter.

I am advised that [INSERT NAME OF PERSON/EVENT/VENUE IMPOSING VACCINE PASSPORTS] (the “**Premises**”) has initiated a policy whereby only those fully vaccinated against SARS-CoV-2 will be granted admission into the Premises and that all persons seeking admission are required to produce certification proving their immunity against SARS-CoV-2 (the “**Policy”).**

The purpose of this communication is to advise you that I believe the Policy being adopted by the Premises represents unnecessary and excessive data collection for which no clear legal basis exists. In support of this position, I say the following:

**1) There is No Legal Basis to Request COVID-19 Vaccination Status Information from Patrons/Others**

On 22 June 2021, the office of the Data Protection Commission published guidance titled: - “*Processing Covid-19 Vaccination Data in the content of Employment*” (the “**2021 Guidance**”). Please be advised that the 2021 Guidance states the following: -

*“As the economy and society continue to open up with the lessening of COVID-19 restrictions, many employers are seeking to understand what information they can process in relation to their employees return to the workplace. In particular, as the rollout of the National Vaccination Programme progresses, the question has been raised as to whether employers can lawfully collect and process information about the COVID-19 vaccination status of their employees.*

*As a general position, the DPC considers that, in the absence of clear advice from public health authorities in Ireland that it is necessary for all employers and managers of workplaces to establish vaccination status of employees and workers, the processing of vaccine data is likely to represent unnecessary and excessive data collection for which no clear legal basis exists. This is particularly the case when there is no public health advice pertaining to what the purpose of such data collection would be. For example, advice as to what employers would be expected to do with knowledge of vaccination status of workers i.e., to send non-vaccinated workers home or segregate vaccinated and non-vaccinated workers in workplaces?*

***Data Minimisation***

*The Work Safely Protocol: COVID-19 National Protocol for Employers and Workers also states that, “Irrespective of the vaccination roll-out, Public Health infection prevention and control measures (such as physical distancing, hand hygiene, face coverings, adequate ventilation), and working from home unless an employee’s physical presence in the workplace is necessary, will all need to remain in place”. This makes it clear that there remains a full suite of measures that employers should employ to maintain workplace safety before considering whether knowledge of vaccination status is a necessary measure. In accordance with the principle of data minimisation, employers should implement all such measures that avoid processing the personal data of employees in the first place.*

***Voluntary Nature of Vaccination***

*Information about a person’s vaccination status is special category personal data for the purposes of the GDPR. It represents part of their personal health record, and is afforded additional protections under data protection law. The Work Safely Protocol: COVID-19 National Protocol for Employers and Workers states that the decision to get a vaccine is voluntary and that individuals will make their own decisions in this regard. This further suggests that COVID-19 vaccination should not in general be considered a necessary workplace safety measure and consequently, the processing of vaccine data is unlikely to be necessary or proportionate in the employment context.”*

Although the 2021 Guidance relates particularly to employment, I am advised that same would likely apply in many other cases where public health authorities in Ireland have not stipulated a requirement that venues establish the vaccination status of patrons/others.

**2) General Data Protection Regulations**

The General Data Protection Regulations (the “**Regulations**”) which came into force on the 25th of May 2018 lay down rules relating to the protection of persons with regard to the processing of their personal data.

The recitals to the Regulations state that: -

 “*The protection of natural persons in relation to the processing of personal data is a fundamental right*”.

Article 8 of the EU Charter of Fundamental Rights states that everyone has the right to the protection of their personal data and such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned, or some other legitimate basis laid down by law.

Information regarding whether or not a patron/other has been vaccinated against SAR-CoV-2 constitutes health data, which is a type of special category data under the Regulations.

**3) Article 6 (Lawfulness of Processing) of the General Data Protection Regulations**

In order to lawfully process health data, you must first determine a legal basis for the processing of such data under Article 6 of the Regulations, which is limited to the following:

* + the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
	+ processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
	+ processing is necessary for compliance with a legal obligation to which the controller is subject;
	+ processing is necessary in order to protect the vital interests of the data subject or of another natural person;
	+ processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
	+ processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

In order to circumvent any suggestion that the Premises may lawfully process my special category data under Article 6 of the Regulations, please note the following:

**3.1 The Data Subject has given Consent to the Processing of his or her Personal Data for One or More Specific Purposes;**

At the outset, I confirm that I do not consent to the processing of my vaccination status by the Premises. In order to pre-empt any suggestion that my refusal to provide any such consent facilitates the Premises in denying me access to the Premises, I wish to draw your attention to the basic requirements for effective valid consent under the Regulations (in circumstances where the Premises seeks to rely on consent as a lawful basis to process any such information).

In this regard I direct you to the following:

* Article 7 (Conditions for Consent) of the Regulations;
* Recital 32 (Conditions for Consent) of the Regulations;
* Recital 42 (Burden of Proof and Requirements for Consent) of the Regulations;
* Recital 43 (Freely Given Consent) of the Regulations; and
* Data Protection Working Party: Guidelines on Consent under Regulation 2016/670 - Adopted on 28 November 2017.

For the sake of completeness, I detail the conditions and requirements of same below.

**Article 7 (Conditions for Consent) of the Regulations provides: -**

*“1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.*

*2. If the data subject’s consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.*

*3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.*

*4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.”*

In particular I draw your attention to the underlined section.

**Recital 32 (Conditions for Consent) provides: -**

*“Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject’s agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject’s acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject’s consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.”*

In particular I draw your attention to the underlined section.

**Recital 42 (Burden of Proof and Requirements for Consent) provides: -**

*“Where processing is based on the data subject’s consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC¹ a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.”*

In particular I draw your attention to the underlined section.

**Recital 43 (Freely Given Consent) provides: -**

*“In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.”*

In particular I draw your attention to the underlined section.

**Article 29 Data Protection Working Party: Guidelines on Consent under Regulation 2016/670 Adopted on 28 November 2017 (“WP29”) provides: -**

*“Generally, consent can only be an appropriate lawful basis if a data subject is offered control and is
offered a genuine choice with regard to accepting or declining the terms offered or declining them
without detriment. When asking for consent, a controller has the duty to assess whether it will meet
all the requirements to obtain valid consent. If obtained in full compliance with the GDPR, consent
is a tool that gives data subjects control over whether or not personal data concerning them will be
processed. If not, the data subject’s control becomes illusory and consent will be an invalid basis for
processing, rendering the processing activity unlawful.”*

*“3.1. Free / freely given*

*The element “free” implies real choice and control for data subjects. As a general rule, the GDPR
prescribes that if the data subject has no real choice, feels compelled to consent or will endure
negative consequences if they do not consent, then consent will not be valid. If consent is bundled
up as a non-negotiable part of terms and conditions it is presumed not to have been freely given.
Accordingly, consent will not be considered to be free if the data subject is unable to refuse or
withdraw his or her consent without detriment. The notion of imbalance between the controller
and the data subject is also taken into consideration by the GDPR.”*

*“3.1.1. Imbalance of power*

*Imbalances of power are not limited to public authorities and employers, they may also occur in other situations. As highlighted by WP29 in several Opinions, consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences (e.g. substantial extra costs) if he/she does not consent. Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will.”*

*“3.1.4. Detriment*

*The controller needs to demonstrate that it is possible to refuse or withdraw consent without
detriment (recital 42). For example, the controller needs to prove that withdrawing consent does not lead to any costs for the data subject and thus no clear disadvantage for those withdrawing consent.*

*Other examples of detriment are deception, intimidation, coercion or significant negative
consequences if a data subject does not consent. The controller should be able to prove that the data subject had a free or genuine choice about whether to consent and that it was possible to withdraw consent without detriment.*

*If a controller is able to show that a service includes the possibility to withdraw consent without any
negative consequences e.g. without the performance of the service being downgraded to the
detriment of the user, this may serve to show that the consent was given freely.”*

With regard to the processing of special category data on the basis of consent, it is undeniable that the element “*free”* implies a real choice by the data subject and any element of inappropriate pressure or influence which could affect the outcome of that choice renders the consent **invalid**. It is also clear that the drafters of the Regulations exercised consideration regarding the possible and sometimes probable imbalance between the controller and the data subject, not only in the context of employment but also as in the present case, where the provision of services/access to premises are based on a data subject providing consent.

**3.2** **Processing is Necessary for the Performance of a Contract to which the Data Subject is Party or in Order to Take Steps at the Request of the Data Subject Prior to Entering into a Contract;**

Article 29 Data Protection Working Party: Guidelines on Consent under Regulation 2016/670 Adopted on 28 November 2017 (“**WP29**”) provides: -

*“3.1.2. Conditionality*

*To assess whether consent is freely given, Article 7(4) GDPR plays an important role. Article 7 (4) GDPR indicates that, inter alia, the situation of “bundling” consent with acceptance of
terms or conditions, or “tying” the provision of a contract or a service to a request for consent to
process personal data that are not necessary for the performance of that contract or service, is
considered highly undesirable. If consent is given in this situation, it is presumed to be not freely
given (recital 43). Article 7(4) seeks to ensure that the purpose of personal data processing is not
disguised nor bundled with the provision of a contract of a service for which these personal data are
not necessary. In doing so, the GDPR ensures that the processing of personal data for which consent
is sought cannot become directly or indirectly the counter-performance of a contract. The two
lawful bases for the lawful processing of personal data, i.e. consent and contract cannot be merged
and blurred.*

*Compulsion to agree with the use of personal data additional to what is strictly necessary limits data
subject’s choices and stands in the way of free consent. As data protection law is aiming at the
protection of fundamental rights, an individual’s control over their personal data is essential and
there is a strong presumption that consent to the processing of personal data that is unnecessary,
cannot be seen as a mandatory consideration in exchange for the performance of a contract or the
provision of a service.

Hence, whenever a request for consent is tied to the performance of a contract by the controller, a
data subject that does not wish to make his/her personal data available for processing by the
controller runs the risk to be denied services they have requested.

To assess whether such a situation of bundling or tying occurs, it is important to determine what the
scope of the contract or service is. According to Opinion 06/2014 of WP29, the term “necessary for
the performance of a contract” needs to be interpreted strictly. The processing must be necessary to
fulfil the contract with each individual data subject. This may include, for example, processing the
address of the data subject so that goods purchased online can be delivered, or processing credit
card details in order to facilitate payment. In the employment context, this ground may allow, for
example, the processing of salary information and bank account details so that wages can be paid.
There needs to be a direct and objective link between the processing of the data and the purpose of
the execution of the contract.*

*If a controller seeks to process personal data that are in fact necessary for the performance of a
contract, it is likely that the correct lawful basis is Article 6(1b) (contract). In this case, there is no
need to use another lawful basis, such as consent, and Article 7(4) does not apply. As the necessity
for performance of contract is not a legal basis for processing special categories of data, this is
especially important to note for controllers processing special categories of data*

*The choice of the legislator to highlight conditionality, amongst others, as a presumption of a lack
of freedom to consent, demonstrates that the occurrence of conditionality must be carefully
scrutinized. The term “utmost account” in Article 7(4) suggests that special caution is needed from
the controller when a contract/service has a request for consent to process personal data tied to it.
As the wording of Article 7(4) is not construed in an absolute manner, there might be very limited
space for cases where this conditionality would not render the consent invalid. However, the word
“presumed” in Recital 43 clearly indicates that such cases will be highly exceptional*

*In any event, the burden of proof in Article 7(4) is on the controller. This specific rule reflects the
general principle of accountability which runs throughout the GDPR. However, when Article 7(4)
applies, it will be more difficult for the controller to prove that consent was given freely by the data
subject.

When assessing whether consent is freely given, one should not only take into account the specific
situation of tying consent into contracts or the provision of a service as described in Article 7(4).
Article 7(4) has been drafted in a non-exhaustive fashion by the words “inter alia”, meaning that
there may be a range of other situations which are caught by this provision. In general terms, any
element of inappropriate pressure or influence upon the data subject (which may be manifested in
many different ways) which prevents a data subject from exercising their free will, shall render the
consent invalid.”*

It is clear from the above, that the Premises cannot rely on Necessity in the Performance of a Contract, as a lawful basis to process special category data.

**3.3 Processing is Necessary for Compliance with a Legal Obligation to which the Controller is Subject;**

Please be advised that the only premises entitled, at law, to impose restrictions upon entry to an indoor premises (on the basis of a person’s vaccination status) are those set out under:

* the Health (Amendment) (No. 2) Act 2021; or
* Statutory Instrument 385 of 2021.

For the avoidance of doubt, a “*relevant indoor premises*” means an indoor premises:

* on or at which food or non-alcoholic beverages may be lawfully sold or supplied for consumption on such premises;
* any business or service that would otherwise be lawfully permitted to sell alcohol for consumption on the premises; and
* such other indoor premises, or class of indoor premises, that the Minister for Health may prescribe through regulations.

It is clear from the above, that the Premises cannot rely on a Legal Obligation as a lawful basis to process special category data.

**3.4 Processing is Necessary in Order to Protect the Vital Interests of the Data Subject or of Another Natural Person;**

The Data Protection Commission Guidance Note: Legal Bases for Processing Personal Data dated December 2019 (the “**2019 Guidance**”) provides the following: -

*“Controllers are most likely to rely on this legal basis where the processing of personal data is needed in order to protect someone’s life, or mitigate against a serious threat to a person, for example a child or a missing person.*

*Vital interests may be an appropriate legal basis in atypical circumstances, where none of the other legal bases clearly apply. For example, where sensitive special category personal data is concerned, such as health data – potentially in an emergency situation – vital interests may provide both a legal basis under Article 6, but also an exception from the prohibition of processing such data under Article 9 GDPR. Many cases in which the protection of vital interests is relied upon as a legal basis for
processing are likely to involve special category health data, and Article 9(2)(c) GDPR allows for processing such data where necessary to protect someone’s vital interests; but, this only applies if the data subject is physically or legally incapable of giving consent.*

*Nevertheless, this legal basis will not apply to all situations concerning the health or treatment of a data subject, but only where the processing is necessary to protect vital interests. As such, it is less likely that this legal basis would apply outside of an emergency situation, for instance where medical care has been planned in advance.*

*Reliance on vital interests as a legal basis is less likely to be appropriate for larger scale processing of the personal data of multiple individuals – it’s more likely to be appropriate in individual emergency situations.*

*What are ‘Vital Interests’?*

*Recital 46 GDPR further elaborates on the kinds of situations in which vital interests may
apply, namely where it is “necessary to protect an interest which is essential for the life of the
data subject or that of another natural person” (i.e. a living individual). Thus, vital interests
can be understood as interests essential for the life of a data subject – mainly covering
life-threatening situations, but potentially situations which very seriously threaten the
health or fundamental rights of an individual.*

*For these reasons, and as alluded to above, most cases in which vital interests are the
appropriate legal basis will involve medical or healthcare situations, including people
in vulnerable mental states, and will often involve sensitive, special category data. The
protection of the actual life of the data subject or another individual is most likely to be
the vital interest which is protected by the necessary processing of personal data.”*

It is clear from the 2019 Guidance that reliance on Vital Interest is limited to emergency situations to protect a person’s life (most often the life of the data subject). Furthermore, the 2019 Guidance also confirms that even where reliance on vital interest is possible (which is denied), the exemption under Article 9(2)(c) of the Regulations is only available (to protect someone’s vital interests) where the data subject is physically or legally incapable of giving consent. On the basis of the 2019 Guidance, it is clear that the Premises cannot rely on a Vital Interest as a lawful basis to process special category data.

**3.5 Processing is Necessary for the Performance of a Task Carried Out in the Public Interest or in the Exercise of Official Authority Vested in the Controller;**

The Data Protection Commission Guidance Note: Legal Bases for Processing Personal Data dated December 2019 (the “**2019 Guidance**”) provides the following: -

*“This legal basis is likely to apply to a more limited sub-set of controllers, where it is necessary for them to process personal data to carry out a task in the public interest, or exercise their official authority.*

*Article 6(3) GDPR also sets out that where processing is based on this legal basis, it should be grounded on EU or national law, which meets an objective or public interest and is proportionate and legitimate to the aim pursued. Thus, a controller may rely on this legal basis if it is necessary for them to process personal data either in the exercise of official authority (covering public functions and powers as set out in law) or to perform a specific task in the public interest (as set out in law).*

*This legal basis is most relevant to public authorities, but could also potentially be relied upon by any controller which in some way exercises official authority or carries out a task in the public interest.*

*There does not need to be a specific legal power to process personal data attributed to that controller, but their underlying task, function or power must have a clear basis in EU or Irish law, including common law.*

*What Kinds of Tasks are in the Public Interest?
Section 38 of the 2018 Act contains further detail on processing for a task carried out in the public interest or in the exercise of official authority in Irish law. It states that processing of personal data shall be lawful to the extent that such processing is necessary and proportionate for (a) the performance of a function of a controller conferred by or under an enactment or by the Constitution, or (b) the administration by or on behalf of a controller of any non-statutory scheme,
programme or funds where the legal basis for such administration is a function of a controller conferred by or under an enactment or by the Constitution.*

*Which Controllers Can Rely on this Basis?
Recital 45 GDPR sheds some light on the question of which categories of controllers might rely on this legal basis, and in which circumstances. It notes that it is primarily for specific EU or national law to determine what kind of controller can perform a task carried out in the public interest or exercise official authority.*

*Most commonly, the controller is likely to be a* ***public authority*** *or another natural or legal person* ***governed by public law****…”*

It is clear from the 2019 Guidance that reliance on Public Task i) is intended to apply (in the main) to public authorities; and ii) can only be utilised where the legal basis is grounded on EU or national law. It is therefore clear that the Premises cannot rely on Public Task as a lawful basis to process special category data.

**3.6 Processing is Necessary for the Purposes of the Legitimate Interests Pursued by the Controller or by a Third Party, except where such Interests are Overridden by the Interests or Fundamental Rights and Freedoms of the Data Subject which require Protection of Personal Data, in particular where the Data Subject is a Child.**

Where a data controller seeks to rely on the Legitimate Interests basis, they should be aware that such utilisation brings with it heightened obligations to balance the legitimate interests they are seeking to pursue with the rights and interests of the data subject.

The Data Protection Commission Guidance Note: Legal Bases for Processing Personal Data dated December 2019 (the “**2019 Guidance**”) provides the following: -

*“Controllers who are assessing whether to process data under the legitimate interest legal basis should consider the three elements needed for this legal basis:
 a) identifying a legitimate interest which they or a third party pursue;
 b) demonstrating that the intended processing of the data subject’s personal data is
 necessary to achieve the legitimate interest; and
 c) balancing the legitimate interest against the data subject’s interests, rights, and
 freedoms.*

*As such, legitimate interests is likely to be an appropriate legal basis in cases where controllers process data subjects’ personal data in a way which they would reasonably expect and which would have a minimal impact on their privacy, by virtue of the nature of the processing or safeguards introduced.*

*Where there would be a more than minimal impact on the data subject’s privacy rights, or other rights, freedoms, or interests, it may still be possible to rely on this legal basis, but the legitimate interest being pursued by the controller would need to be a particularly compelling justification for processing.*

*What Kinds of Legitimate Interests Are Covered?
A relevant legitimate interest could, for example, exist in various situations where there is a ‘relevant and appropriate relationship’ between the data subject and the controller, as noted in Recital 47 GDPR. This might apply in situations such as where the data subject is a client or in the service of the controller. The existence of a legitimate interest requires careful assessment, including, in particular, whether a data subject can ‘reasonably expect’ at the time and in the context of the collection of the personal data that processing for that purpose may take place.*

*The GDPR, at Recital 47, gives some more concrete examples of the kinds of interests which might constitute legitimate interests for this purpose, noting that the processing of personal data strictly necessary for the purposes of preventing fraud is likely to constitute such, and even that processing for direct marketing purposes may be regarded as carried out for a legitimate interest.*

*In both cases, particularly the latter, controllers will still need to carefully assess whether the purposes of their intended processing do in fact constitute a legitimate interest, as well as balancing this against the data subject’s interests, as discussed in more detail below.*

*Once a legitimate interest has been identified, a controller must be able to show that the processing of personal data is actually necessary for the purpose of that interest. The necessity test requires controllers to demonstrate that the processing is a reasonable and proportionate way of achieving their purpose. If a controller can reasonably pursue these interests in another, less intrusive way, legitimate interests will not provide a legal basis for processing.

The Balancing Test
As mentioned above, a key component of this legal basis is that it may only be relied upon where the legitimate interests which are pursued by the controller or third party are not overridden by the interests, rights, and or fundamental freedoms of the data subject.*

*As such, controllers need to undertake a balancing exercise when assessing whether the processing of personal data should take place under this legal basis. This exercise should, as noted in Recital 47 GDPR, take into consideration the ‘reasonable expectations’ of data subjects, in the context of their relationship with the controller.

A large part of the balancing test undertaken by controllers should also be based on common sense and the expectations of the data subject: If a data subject would not reasonably expect this type of processing of their personal data, or if it would cause unjustified harm to their interests, rights, or freedoms, their interests are likely to override the legitimate interests upon which the controller is seeking to rely. Similarly the greater the intrusion a certain processing operation has on the data protection rights of an individual, the greater the justification needed to ground that processing.

Thus, where a controller is considering processing personal data based on legitimate interests, they should ensure that they have undertaken the balancing test, and are confident that the data subject’s interests do not override those legitimate interests and that the personal data are only used in ways the data subject would reasonably expect – unless there is a very strong reason overriding these concerns.

Factors which should be considered as part of the balancing test include the circumstances and context of each case, in particular the nature of the personal data and the processing and the relationship between the controller and data subject, but also data protection considerations such as data minimisation, retention periods, safeguards in place, data protection by design and by default, and the existence of clear and accessible opt-out mechanisms.*

*In line with the principle of accountability, found in Article 5 GDPR, controllers should keep a record of the assessment they undertook to* *determine whether the legitimate interests were overridden by the interests, rights, or freedoms of the data subject.”*

Given that the disclosure of special category data to enter a premises or to access goods or services is considered by many to be the most intrusive invasion into the privacy rights of citizens in recent memory, it is clear that reliance on Legitimate Interests would be difficult to justify, given that any justification must be balanced against the fundamental rights of the individual. In circumstances where the Premises intends to endeavour to rely on this basis to process special category data, please furnish a copy of the record of assessment (which predates the implementation of the Policy) which determined that the legitimate interests pursued by the data controller overrides the interests, rights, or freedoms of the data subject.

**4) Article 9 (Processing of Special Categories of Personal Data) of the General Data Protection Regulations**

In circumstances where the Premises can determine a legal basis for the processing of health data under Article 6 (which appears unlikely), then the Premises should be aware that the processing of special categories of personal data (which includes health data) is generally prohibited unless the Premises can avail itself of one of the exemptions under Article 9, which is limited to the following:

* 1. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
* as confirmed above, I do not consent to the processing of my special category data by the Premises.
	1. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
* this exemption is not applicable as my attendance at the Premises is unrelated to employment or social security.
	1. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
* the scope of the exception is limited as it concerns only the protection of a “*vital interest*” of a person, that is to say, “*an interest which is essential for [her/his] life*” (Recital 46 of the Regulations). It includes threats to the physical integrity or life of a person or a third person. In other words, it must be a matter of life and death. The second condition limits drastically the scope of the vital interest’s exception: it may be invoked **only** if the individual is physically or legally incapable of giving consent.
* this exemption is not applicable as the processing is not essential to life and also in light of the fact that I am both physically and legally capable of giving or refusing consent.
	1. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
* this exemption is not applicable as the Premises is not a foundation, association or not-for-profit body with a political, philosophical, religious or trade union aim. Furthermore, even in circumstances where the Premises could argue that it is a foundation, association or not-for-profit body with a political, philosophical, religious or trade union aim – it should be noted that these organizations may **only** process special categories of personal data in the course of their “*legitimate activities*”. This means that the processing must be directly connected to the political, philosophical, religious or trade union activities of the organization. An association, a foundation or any other not-for-profit body cannot invoke this exception to process special categories of personal data that are **not** closely related to its core activities in accordance with its purposes and powers set out in its governing charter.
	1. processing relates to personal data which are manifestly made public by the data subject;
* this exemption is not applicable as I have not manifestly made public the special category data sought by the Premises.
	1. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
* this exemption is only available where the processing is necessary for legal claims and judicial activities, that in many cases **require** the processing of certainly sensitive data, in light of same this exemption is not applicable.
	1. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
* in circumstances where a Premises wishes to avail of the Substantial Interest ground, the Premises would need to be able to substantiate that a substantial public interest requires the processing of such special category data, and in light of the fact that such processing has not been made mandatory in law (with respect to the Premises), in my view it would be difficult to substantiate any such claim.
* in circumstances where the Premises nevertheless seeks to rely on this exemption, I say that this exemption is only open to Premises where the legal basis is grounded on EU or national law.
	1. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
* this exemption is only available if the processing of my vaccination status is necessary for occupational or preventative medicine or for assessing the working capacity of the employee – therefore, this exemption will not be applicable to the vast majority of Premises.
* in circumstances where the Premises nevertheless seeks to rely on this exemption, I say that this exemption is only open to Premises where the legal basis is grounded on EU or national law.
	1. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
* this exemption is not applicable as it is aimed at cross-border threats to health and ensuring high standards of safety of health care, medicinal products, or medical devices. Given that my access into the Premises does not entail the crossing of borders and also in circumstances where all persons crossing the border into Ireland are required, by law, to produce their EU Digital Green Certificate proving their immunity to SARS-CoV-2, I fail to see how this exemption could be open to the Premises.
* in circumstances where the Premises nevertheless seeks to rely on this exemption, I say that this exemption is only open to Premises where the legal basis is grounded on EU or national law.
* finally, if a Premise wishes to avail of this exemption, it should be noted that any such Premises is required to put in place appropriate measures and safeguards to protect the rights and freedoms of the data subject. Furthermore, with respect to this exemption, the request and processing of my vaccination status can only be carried out by a health professional or someone else who owes a legal duty of confidentiality.
	1. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with [Article 89](https://gdpr-info.eu/art-89-gdpr/)(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
* this exemption is not applicable as the processing of my special category personal data is not sought for the purposes of i) archiving in the public interest; ii) scientific or historical research purposes; or iii) statistical purposes.

**5) Data Protection Impact Assessment**

Article 35 (Data Protection Impact Assessment) of the Regulations states: -

*“1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks….*

*3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: …. (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10;”*

**6) In light of the above, I would be grateful for your response to the following questions in order that I may determine whether a complaint should be made to the Data Commissioner regarding your Vaccination Status Policy:**

* Please provide the legal basis upon which the collection and processing of my special category data is considered lawful under Article 6 of the General Data Protection Regulations.
* Please provide the legal basis upon which the collection and processing of my special category data is considered lawful under Article 9 of the General Data Protection Regulations.
* In circumstance where you consider that there is a lawful basis to process my special category data under 6 and 9 of the General Data Protection Regulations, please advise what the purpose of such data collection is.
* Please provide a copy of the Data Protection Impact Assessment required under Article 35 of the Regulations.
* In circumstances where the Premises intends to endeavour to rely on the Legitimate Interest basis to process special category data, please furnish a copy of the record of assessment (which predates the implementation of the Policy) which determined that the legitimate interests pursued by the data controller overrides the interests, rights, or freedoms of the data subject.

**7) Refusal of Admission into a Premises / Access to Goods or Services amounts to Discrimination under the Equal Status Acts**

Section 5(1) of the Equal Status Acts stipulates that a person shall not discriminate in disposing of goods or services to the public generally or a section of the public. Section 3(2)(g) of the Equal Status Acts, states that an act of discrimination occurs if a person is treated less favourably on the basis of nine protected grounds which includes: gender, marital status, family status, age, disability, sexual orientation, race, religion, and membership of the Traveller community.

An argument could be advanced by “*relevant indoor premises”* that they were required, by law, to implement the discrimination set out under the Health (Amendment) (No.2) Act 2021 and in certain circumstances this may act as a shield against any legal challenge citing discrimination, however, given that the Premises is not protected (in any way) by the Health (Amendment) (No.2) Act 2021, the Premises is fully exposed to a claim for discrimination under the Equal Status Acts given that they are treating less favourably persons who are not vaccinated against SARS-Cov-2, as against persons who are vaccinated against SARS-CoV-2.

Furthermore, given that there is no lawful basis to process vaccination status information, it naturally follows, that there is no lawful basis to enquire into a persons possible protected status under the Equal Status Acts as divulging any such information would naturally disclose whether a person has been vaccinated against SARS-CoV-2.

**8) Required Actions**

Please be advised that failing a reversal of the Policy, I intend to consult with a legal advisor in connection with the initiation of legal proceedings and/or the submission of a complaint to the Data Commissioner on the basis of:

1. The unlawful processing of special category data under the General Data Protection Regulations;
2. The failure by the Premises to complete (in advance) a Data Protection Impact Assessment as required under Article 35 of the General Data Protection Regulations.
3. Discrimination under the Equal Status Acts;

Please be advised that the Data Commissioner has the authority under the Regulations to issue fines of up to €20m or 4% of your global turnover (whichever is higher) for severe breaches of data protection, and up to €10m or 2% of global turnover (whichever is higher) for less severe breaches. It should also be noted that the Data Commissioner has issued a total of €715,000 in fines under these regulations since May 2018, with fines under the Regulations jumping 40% in the past year by regulators throughout the EU.

Given the seriousness of this matter and the fact the Premises should have considered all of the matters raised in this correspondence prior to the inception of the Policy, I require a reasoned response within 7 days from the date hereof, or alternatively confirmation that you have reversed your Policy and will no longer discriminate against persons not vaccinated against SARS-CoV-2.

Yours sincerely,

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
[INSERT YOUR NAME AND ADDRESS]