

SONY MUSIC ENTERTAINMENT

PRIVACY POLICIES AND OPT-IN PROCEDURES FOR ASIA AND MIDDLE EAST

EXECUTIVE SUMMARY

- A privacy policy and its accompanying opt-in procedure are the method by which Sony Music Entertainment (“**SME**”) complies with its legal obligations to notify and obtain the consent of consumers to the collection and processing of their personal data.
- Whilst different jurisdictions will reflect local cultures and practice, there are certain mandatory provisions that must be reflected in the privacy policy to ensure that SME can use personal data in the commercial manner it desires.
- As a general rule, if a consumer is not informed of an intended purpose for their data, then it cannot be used for that purpose. Note certain intended uses of personal data (e.g. the transfer of data out of data user’s home territory) may require other strict conditions to be satisfied.
- The privacy policy and opt-in language should be clearly accessible at the point at which a consumer’s personal data is collected. The privacy policy should also be accessible from at least the homepage of the website (and, ideally, from any page).

1. INTRODUCTION

All websites (whether generic or artist, and whether managed by SME, an artist or a third party) must contain a privacy policy.

In most cases, typically where downloads or other products can be purchased or where users are able to post material online, the website should also have ‘terms and conditions of use’ (including, for instance, limitations of liability for content of other websites, competition terms, etc) – although this should be separate from, and not merged with, the privacy policy . A privacy policy explains to website users (“**data subjects**”) how their data is collected and used. The content of the privacy policy is guided by data protection law at local country level, with local regulators exercising different levels of scrutiny over business practices.

The privacy policy is the primary means by which SME ensures that its collection and processing of data is carried out in accordance with the general core principles prescribed in a number of Asian and Middle East territories (e.g. that data should be processed fairly and lawfully, that it should be collected and used only for specific purposes, that the data should be adequate, relevant and not excessive in relation to the purposes, etc).

Accordingly, in order to ensure that we are able to use the data we collect in the manner we desire, we must obtain the corresponding degree of informed consent from the consumer. The two ways in which we satisfy our legal obligations are by ensuring (i) that our privacy policies comply with some basic levels of content and (ii) that our consumers are given sufficient information to ‘opt-in’ to the processing of their data we intend to carry out are.

2. MANDATORY NOTICE PROVISIONS IN PRIVACY POLICIES

(a) The identity of the data user

The privacy policy must clearly state the details of the corporate entity that will determine the purposes and means of processing a consumer’s personal data (the “**data user**”). This data

user will nearly always be an SME company. Where a third party is engaged to process data on behalf of the data user, that body is known as the “data processor”.¹ This may be the case where a third party hosts or manages a website on behalf of SME. Whatever the particular circumstances, the full identity of the data user (including full registered company name, number and postal address) must be made explicit.

(b) The purpose(s) for which the data is being collected

The policy must set out the purposes for which the personal data being collected. There must be a sufficient level of specificity, rather than just vague, general statements.

(c) Recipients of the data

The privacy policy should set out with whom the data user will share the data. The policy must state that data may be shared globally (see (d) below) with our group companies / affiliates, service providers, artists (including management) and due to corporate transactions. The possibility of special circumstances (e.g. disclosure required by law) should be mentioned. In each case, the sharing is subject to two important conditions: the transfer of data out of the data user’s home territory and the data subject’s informed consent (via an opt-in).

(d) The transfer of data out of data user’s home territory

Some Asian (and Middle East) territories prohibit the transfer of data out of the data user’s home territory unless either (i) measures are put in place to ensure that protection similar to the local level is granted, (ii) such transfer is *necessary* (not desirable) for a number of specified purposes (e.g. public interest grounds) or (iii) the data subject’s unambiguous consent to the transfer has been obtained. The privacy policy should, therefore, state that SME will only transfer data of the data user’s home territory where it can do so lawfully - and state that such transfer may be worldwide.

(e) Children

While a number of data protection laws in Asia and Middle East are not specific on the issue of children’s personal data, SME’s global policy is not to collect the personal data of children under the age of 13. However, should your local data protection laws or best practice require particular procedures or have more strict requirements, please ensure that these are reflected in your policy and opt-in.

(f) The use of ‘cookies’

Where data is being collected by the use of ‘cookies’, the privacy policy should explicitly state so. It should also explain what a ‘cookie’ is and inform the data subject that they can adjust their browser (but that that might affect their access to the full functionality of the site).

(g) The existence of the right of access and rectification

The privacy policy must inform the data subject that they have the right of access to their own data and the right to rectify such data, and then set out how those rights can be exercised.

3. THE LOCATION OF THE PRIVACY POLICY

Regulatory best practice dictates that a privacy policy “*should be directly accessible on the home page of the site and anywhere where personal data are collected online.*” In practice, at the time when a user registers on the site, the privacy policy should be clearly and

¹ there may be certain requirements which must be met when outsourcing data processing to a third party.

explicitly referred to, with clear opt-in language and provisions to ensure informed consent is obtained.

4. SHARING OF DATA WITH/FROM THIRD PARTIES

Where SME is to receive data from, or share data with, third parties, care must be taken to ensure that the consumer is specifically made aware of, and consents to, such sharing. For example, where a third party partner is collecting data and intends to share it with SME, that third party's privacy policy should include wording to that effect.

Note that data received from third parties can only be used in accordance with the purposes that the consumer was informed of at the time their data was originally collected.

5. OPT-IN PROCEDURES

It is a general principle of data protection laws in Asia (and probably in Middle East) that a data subject's consent must be "*freely given, specific and informed.*"

Although the legal position is not entirely clear, there appears to be a broad consensus that simply making a link to a privacy policy available somewhere on the site is not sufficient to obtain such informed consent from a consumer. Similarly, some of the intended use of the data (e.g. sharing of data with third parties) is such that it should be specifically drawn to the attention of the data subject before any such processing can lawfully occur.

Local regulation and best practice will dictate the exact opt-in procedure and language (particularly if there are specific requirements with respect to children – see para 2(e) above). However, an example of suitable opt-in language at the time of registering on the site is:

"I have read and understood the privacy policy² and agree to the processing of my data in accordance with it."

² The words 'privacy policy' should include a hyperlink to the text of the underlying privacy policy itself.