**NMT HR SERVICES LTD**

**CHECKLIST FOR ENSURING LAWFUL BASIS - CONSENT**

**Checklist – asking for consent**

☐ We have checked that consent is the most lawful basis for processing

☐ We have made the request for consent prominent and separate from our terms and conditions

☐ We ask people to positively opt in

☐ We don’t use pre-ticked boxes or any other type of default consent

☐ We use clear, plain language that is easy to understand

☐ We specify why we want the data and what we are going to do with it

☐ We give individual options to consent separately to different purposes and types of processing

☐ We name our organisation and any third-party controllers who will be relying on the consent

☐ We tell individuals that they can withdraw their consent

☐ We ensure individuals can refuse to consent without detriment

☐ We avoid making consent a pre-condition of a service

☐ If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental consent measures for younger children in place)

**Checklist – recording consent**

☐ We keep a record of when and how we got consent from the individual

☐ We keep a record of exactly what they were told at the time

**Checklist – managing consent**

☐ We regularly review consents to check that the relationship, the processing and the purpose have not changed

☐ We have processes in place to refresh consent at appropriate intervals, including parental consents

☐ We consider using privacy dashboards or other preference-management tools as a matter of good practice

☐ We make it easy for individuals to withdraw their consent at any time, and publicise how to do so

☐ We act on withdrawals of consent as soon as we can

☐ We don’t penalise individuals who wish to withdraw consent

**Please note:**

* The GDPR sets a high standard for consent. But you often won’t need consent. If consent is difficult, look for a different lawful basis
* Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build customer trust and engagement, and enhance your reputation
* Check your consent practices and your existing consents. Refresh your consents if they don’t meet the GDPR standard
* Consent requires a positive opt-in. Don’t use pre-ticked boxes or any other method of default consent
* Explicit consent requires a very clear and specific statement of consent
* Keep your consent requests separate from other terms and conditions
* Be specific and ‘granular’ so that you get separate consent for separate things. Vague or blanket consent is not enough
* Be clear and concise
* Name any third-party controllers who will rely on the consent
* Make it easy for people to withdraw consent and tell them how
* Keep evidence of consent – who, when, how, and what you told people
* Keep consent under review, and refresh it if anything changes
* Avoid making consent to processing a precondition of a service
* Public authorities and employers will need to take extra care to show that consent is freely given, and should avoid over-reliance on consent

**How should you obtain, record and manage consent?**

Make your consent request prominent, concise, separate from other terms and conditions, and easy to understand. Include:

* the name of your organisation;
* the name of any third-party controllers who will rely on the consent;
* why you want the data;
* what you will do with it; and
* that individuals can withdraw consent at any time

### What is valid consent?

Consent must be freely given; this means giving people genuine ongoing choice and control over how you use their data.

Consent should be obvious and require a positive action to opt in. Consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand, and user-friendly.

Consent must specifically cover the controller’s name, the purposes of the processing and the types of processing activity.

Explicit consent must be expressly confirmed in words, rather than by any other positive action.

There is no set time limit for consent. How long it lasts will depend on the context. You should review and refresh consent as appropriate.

**What are the key changes to make in practice?**

You will need to review your consent mechanisms to make sure they meet the GDPR requirements on being specific, granular, clear, prominent, opt-in, documented and easily withdrawn.

The key new points are as follows:

• ***Unbundled***: consent requests must be separate from other terms and conditions. Consent should not be a precondition of signing up to a service unless necessary for that service.

• ***Active opt-in***: pre-ticked opt-in boxes are invalid – use unticked opt-in boxes or similar active opt-in methods (e.g. a binary choice given equal prominence).

• ***Granular***: give granular options to consent separately to different types of processing wherever appropriate.

• ***Named***: name your organisation and any third parties who will be relying on consent – even precisely defined categories of third-party organisations will not be acceptable under the GDPR. • ***Documented***: keep records to demonstrate what the individual has consented to, including what they were told, and when and how they consented.

• ***Easy to withdraw***: tell people they have the right to withdraw their consent at any time, and how to do this. It must be as easy to withdraw as it was to give consent. This means you will need to have simple and effective withdrawal mechanisms in place.

• ***No imbalance in the relationship:*** consent will not be freely given if there is imbalance in the relationship between the individual and the controller – this will make consent particularly difficult for public authorities and for employers, who should look for an alternative lawful basis.