

# Recruiters & HR & PII! Oh My!

Where has all ~~my~~  
personal information  
gone?





# Why recruiters & HR are targets

**A lot of personal information is collected during the hiring process, making recruiters and HR departments prime targets for threat actors.**

**And a lot of this data is ~~protected~~ under Australian privacy law!**



# The Privacy Act

The Australian Privacy Act has an exemption for employee data, but only for **existing and past** employees.

RESUME

It does **not** cover candidates you never hired, or have not yet hired!



# **What personal information?**

**Personal information collected during hiring can include:**

- 1. Resumes**
- 2. Tertiary education certificates**
- 3. Marriage certificates**
- 4. Birth certificates**
- 5. Passports**
- 6. Drivers licenses**
- 7. Superannuation information**
- 8. Tax file numbers (TFN)**



# Recruiter Obligations

**You are obligated under the Australian Privacy Act to protect ~~all~~ candidate personal information from disclosure.**

**No candidates become your employees so their personal information is ~~not~~ exempt!**



# HR Obligations

**You are obligated under the Australian Privacy Act to protect personal information for candidates during the hiring process, and any that were not employed after the hiring process.**

**Only ~~existing~~ and ~~past~~ employee's data is exempt.**



**So what can  
I do to protect  
my candidate's  
personal  
information?**



**1**

# **Awareness Training**

**Conduct regular security awareness training which covers:**

- 1. Latest threat actor tactics, so you know what to look for**
- 2. What your company is doing to keep data safe**
- 3. What is expected of you to help protect this information**





2

## Limit Storage of Data

**Only store information you actually need.**

**Delete information as fast as possible once it is not needed.**

**Automate this process if you can.**



3

## Use MFA

Use multi-factor authentication (MFA) on **all** systems, especially any that hold personal information.





4

## Know where your data is

**Know** where your data is and ensure only those who **need** access can access it.

**Limit the number of places personal information is stored to reduce your attack footprint.**



5

## Don't collect data you don't need

Let candidates know what  
information ~~not~~ to send you.

If you never receive the data,  
you don't need to protect  
it.



6

## Understand the impact

Understand ~~why~~ protecting candidate data is so important and how it can have an enormous personal impact on them if you are breached.

And understand the impact it would have on ~~your~~ organisation as well.



# Want More Information?

**Read more on our blog  
about your obligations,  
what you can do,  
and if you need help,  
our service that helps  
recruiters and HR.**

<https://morrisec.com.au/insights>



**MORRISEC**