

## **Former Employee Fined for Data Breach: What Your Business Can Learn**

A recent case involving a former employee of Enterprise Rent-A-Car highlights the importance of robust data protection measures.

Jonathan Riches was fined £10,000 and ordered to pay £1,700 in costs after pleading guilty to illegally accessing motorists' personal details. This breach involved Mr Riches using his former connections at Enterprise to obtain sensitive data for personal injury claims.

The case underscores the importance of maintaining strong data security procedures for employee access to business systems.

So, what can your business learn from this? Here are some key takeaways to help you avoid a similar situation:

### **1. Strengthen access controls:**

Sensitive data should only be accessible to employees who need it. Therefore, regularly review who has access and update permissions as and when roles change within your business.

### **2. Implement robust data security policies:**

Having clear and comprehensive data protection policies in place is essential. These policies should be

communicated to all employees, who will need regular reminders to ensure that everyone understands their role in protecting client information.

### **3. Monitor and audit access:**

Your systems should be capable of monitoring who is accessing your data and you should arrange for regular audits to be carried out. This can help you spot any unauthorised access early and take immediate action.

### **4. Effective employee offboarding:**

When an employee leaves your company, it's vital to revoke their access to your business systems and data immediately. This step helps prevent any potential misuse of information after their departure.

### **5. Prompt reporting and response:**

If a data breach does occur, you should report it to the appropriate authorities immediately. Having a clear action plan in place ensures you can respond quickly so that you can minimise any damage caused and protect your business.

By taking these proactive measures, you can better safeguard your business against data breaches and avoid the legal and financial repercussions that come with them.

Ensuring your data protection practices are up to date not only protects your clients but also strengthens your business's reputation and trustworthiness.