

without authorisation, copying 640 files of KXS's confidential information onto a personal hard drive on his last day of employment.

[3] KXS further claims that NXJ breached confidentiality obligations by during, and following, employment, disclosing and sharing KXS's Human Resources (HR) documentation with his network of HR professionals and private HR consultancy clients.

[4] NXJ denies that he breached any confidential obligation owed to KXS by copying any files from his work laptop to a personal external hard drive during his employment. He claims there was no requirement of his employment that he did not copy files.

[5] NXJ further claims that KXS has not been able to identify any material consequence for it, or actual harm caused to it since his employment ended on 31 January 2022.

Non Publication Order

[6] **Pursuant to clause 10 (1) of Schedule 2 of the Act, the names of the Applicant and the Respondent, and any identifying details are prohibited from publication until this order is revoked or varied by further orders of the Authority. They will be identified only by randomised initials which have no correlation to their actual names.**

The Authority's investigation

[7] During the Investigation Meeting, NXJ and General Counsel of KXS, who had provided written affidavits, answered questions under oath or affirmation from the Member and under cross-examination. Counsel for the parties provided written and oral submissions.

[8] As permitted by s174E of the Employment Relations Act 2000 (the Act) this determination has stated findings of fact and law, expressed conclusions on issues necessary to dispose of the matter and specified orders made. It has not recorded all evidence and submissions received.

Issue

[9] This preliminary determination determines whether or not a witness summons should be issued requiring NXJ to provide all relevant devices held by him to be made available for examination by an independent forensic examiner.

Brief Background

[10] KXS is a technology provider. It employs approximately 520 employees in New Zealand.

[11] NXJ was employed by KXS in the position of Chief People Officer, People & Capability, on 17 January 2019. His employment ended on 31 January 2022 (with a one week extension).

[12] NXJ said that during the recruitment process, he notified KXS of various interests that he held in other entities, including ongoing consultancy work.

[13] KXS said that NXJ promised he would immediately raise any conflicts of interest that arose and resolve them in a way that did not disadvantage KXS.

[14] The employment agreement dated 2 November 2018 (the Employment Agreement) includes the following clause:

14. Termination of Employment

14.6 Upon termination of employment for whatever reason the Employee will immediately deliver to KXS:

- (a) documents, letters, papers, business cards and other material of every description (including computerised records and copies of or extracts from the same) within the Employee's possession or control relating to the affairs and business of or belonging to KXS; and
- (b) all equipment or other property (including, for example, keys, access cards, laptop computer, cell phone, credit card) of KXS prior to the payment of the Employee's final salary entitlement. If the equipment or other property is not returned or is damaged, KXS may make a rateable deduction from the Employee's final pay including holiday pay for the cost of repair or replacement of the equipment or properly.

[15] In Schedule 3 of the Employment Agreement headed 'Background, Confidential Information, Intellectual Property and Restrictive Covenants' it states :

1.1 For the purposes of this provision:

...

(b) "Confidential Information" includes:

- (i) information which by its nature or notice is intended for limited distribution within KXS;
- (ii) sensitive information which constitutes or relates to KXS's records or business affairs; for example vendor lists, customer lists, pricing information and information contained in internal correspondence, reports, memoranda, and other documents in whatever form which is utilised internally by KXS in the conduct of its business; or constitutes or relates to

confidential information provided to KXS by third parties such as KXS vendors', licensors' or customers' drawings, specifications, plans, proposals, programs, formulas, Inventions, devices, methods, techniques, patterns, processes, lists and compilations of information which are maintained by KXS for its own private use, whether or not specifically marked as Trade Secret or Confidential;

(iii) information belonging to or in the possession of KXS which:

(aa) derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and

(bb) is the subject of efforts that are reasonable to maintain its secrecy.

1.3 The Employee shall not disclose, use or engage in behaviour likely to result in the disclosure or use of any Confidential Information for so long as such Confidential Information is not generally known to the public, except as may be required by lawful order of a court or as authorised in writing by KXS, whether during the employment or after the end of it, and whether the Employee resigns or is dismissed by KXS,

[16] During his employment with KXS, NXJ provided HR services to his own private clients. He was also part of a network of HR Professionals which shared documents with each other on a confidential basis including research, policies and templates.

[17] On 14 October 2021 the parties entered into a Record of Settlement pursuant to s 149 of the Employment Relations Act 2000 (the Act). The Record of Settlement recorded that the parties agreed NXJ's employment would end on 31 January 2022. The Record of Settlement contained the following clauses:

10. One or before the Termination Date, the Employee is to return all of the information and property belonging to the Employer and its related companies that is in the Employee's possession including, without limitation, laptop, mobile phone, credit cards, swipe cards, any demonstration units, and any confidential information held in whatever form (including in electronic form on any device or web based application). The Employee agrees not to retain any copies. Copies include soft copies stored on computers, devices or otherwise in the Employee's possession or control (including in the cloud).
13. All of the Employee's obligations in the employment agreement between the Employer and Employee, which survive the termination of employment, remain in full force and effect.
 - b) The Employee will not disclose to any person any confidential information concerning any matter relating to the business or affairs of the Employer or its directors, officers, agents, employees or customers which confidential information has been acquired by the

Employee in the course of his employment, unless such information comes into the public domain otherwise than by a breach of confidence on the part of the Employee;

- c) For the purposes of clause 14(b), “confidential information” means any information of a confidential or secret nature relating to any and all aspects of the Employer including but not limited to:
 - i. information relating to the Employer’s products, processes and procedures;
 - ii. customer information;
 - iii. financial information, budgets, reports, business plans, strategies, know-how, pricing and sales and marketing plans.

[18] Although NXJ’s termination of employment was recorded as 31 January 2022, he was placed on garden leave on 17 December 2021.

[19] KXS claims that on NXJ’s last day of employment, 31 January 2022, he copied 640 files from his work laptop onto an external storage device. KXS had not given authorisation for NXJ to do this. The General Manager said the files copied included:

- a. HR policies and templates;
- b. Board papers, plans, strategy documents and reports;
- c. Salary, performance and other employment information (including CVs, offers of employment, terms and conditions of employment and records of settlement) for former and current employees of KXS.

[20] NXJ confirmed that he did copy a large number of files immediately prior to the termination of his employment to ensure that he did not lose any personal files and to ensure KXS did not retain access to confidential information that did not belong to it.

[21] NXJ’s evidence was that whilst he was on garden leave he ran out of time to remove his personal information from his work computer. The personal information files were not in a discrete file on his computer and were not easily identifiable. He requested, and was granted, continued access to KXS’s systems following the termination of his employment.

Events March 2022

[22] KXS engaged a company, InPhySec to assist it with cybersecurity, providing it with a monthly report. On 1 March 2022, as a result of the monthly report, KXS’s Head of IT discovered the file copying carried out by NXJ on his last day of employment.

[23] KXS's Head of IT assumed NXJ had copied the files for the purpose of a handover with his successor and did not take any further action until 25 March 2022.

[24] However on that date he checked if the files had been used in a handover with NXJ's successor, and on receiving a negative, had escalated the matter to KXS's General Manager (now Chief Executive Officer) who asked for more information on the downloaded files.

[25] The General Manager explained that KXS had been concerned about its privacy obligations in light of NXJ having downloaded current and former employees' personal information. As a result, on 14 April 2022 KXS notified the Office of the Privacy Commission of the data breach.

[26] On 29 April 2022 KXS wrote to NXJ requesting that (i) he agree to a forensic review process at his cost in order to identify and remove its information; and (ii) he provide a statutory declaration about what he had done with the information he had copied.

[27] NXJ responded on 6 May 2022 explaining that he had copied the files because of the intermingling of KXS files with his personal files and had permanently deleted all KXS files from the external hard drive.

[28] KXS did not respond to NXJ's email until 27 May 2022 due to the Acting CEO being away from the office. In that email KXS reiterated that it wanted NXJ to comply with its request for a forensic examination process.

[29] NXJ said that before receiving this email from KXS he destroyed the hard drive onto which he had transferred the files by drilling it with a steel bit, then throwing it away in his household rubbish collection.

[30] KXS's evidence is that NXJ subsequently changed his explanation of the reason he took the files, repeatedly refused to agree to a forensic retrieval process and to provide the statutory declaration in the form it requested.

Should a witness summons be issued requiring NXJ to provide all relevant devices for forensic examination?

Applicant's submissions

[31] It is submitted for KXS that without the forensic search orders, the Authority is unable to investigate its claims because NXJ possesses relevant material on his computer systems. It is submitted that the relevant missing evidence only on NXJ's computer systems is:

- a) Evidence, or a lack thereof, of any documents on NXJ's devices and platforms which either are KXS's documents, or documents created using KXS's confidential and proprietary information;
- b) Metadata within his cloud-based storage accounts/email accounts/local servers and hard drives that would show whether KXS's information has ever been saved there, and if so, what happened to it; and
- c) Metadata within his laptop and any other personal devices that would show whether NXJ plugged in the hard drive for the purpose of transferring the personal files and any other of NXJ's documents to his other systems, and what happened to that information once it was transferred off the hard drive.

[32] It is further submitted that without reviewing NXJ's computer systems with the assistance of an IT expert, the Authority will have no way to establish whether or not NXJ has breached his obligations because relevant evidence will not be examined.

[33] It is submitted that KXS does not trust NXJ to comply with his obligations on the basis that:

- a) NXJ has admitted not keeping to commitments in his employment agreement and the Record of Settlement, referred to by NXJ as "technical breaches";
- b) NXJ's explanations for copying the 640 files have been implausible and inconsistent, heightening KXS's concerns.
- c) NXJ refused a forensic examination when requested, providing instead carefully worded undertakings regarding his information and has still not provided a sworn statutory declaration. Although it is acknowledged by KXS that NXJ offered a statutory declaration on 20 March 2023 which covered misuse and third party transfers:

- i. That declaration has not been provided as yet; and

- ii. Even if a statutory declaration was provided KXS does not accept that NXJ properly understands what is and is not confidential information, and what constitutes misuse. On that basis such a statutory declaration would be unreliable.
- d) NXJ did not disclose the fact that he had destroyed the hard drive with a steel drill until the Authority's investigation meeting;
- e) NXJ does not understand the privacy implications of his actions.

[34] Finally it is submitted that NXJ will not be prejudiced if the orders sought by KXS are granted because the Orders provided by the Authority will have safeguards built into them.

Respondent's submissions

[35] It is submitted for NXJ that a forensic examination has only very limited relevance and is of no real value to KXS's business. It is submitted that even if a forensic investigation did identify any misuse of KXS's information for the benefit of NXJ's own business, any such misuse can have caused KXS only nominal harm. Moreover KXS has not been able to identify any material harm caused.

[36] In support it is submitted that NXJ's employment ended on 31 January 2022 and that if any actual harm had been caused to KXS by NXJ's actions, KXS would have been aware of it by now. As such it is submitted that a forensic examination is disproportionate and unreasonable.

[37] NXJ has admitted to KXS that he committed a minor technical breach of his obligations by not ensuring that all company property was returned to it, and that all copies of company property held by him were not destroyed or deleted on or before the end of his employment. It is submitted that this has now been done, however it was not designed to cause KXS any harm, and in fact has not done so.

[38] NXJ does not consider that a forensic investigation into all his computers, phones, email and online accounts to be reasonable on the basis that he has not disclosed or misused any confidential information belonging to KXS and has provided an undertaking to this effect.

[39] It is submitted that the argument that NXJ took the information deliberately and with the intention of using it for his own benefit is implausible because the information has no value to him. It is irrelevant to NXJ's HR Consultancy work, the business of his clients, and his new employer.

[40] It is submitted that NXJ copied the files immediately prior to the termination of employment to ensure he did not lose personal files and to ensure that KXS did not retain access to confidential information that did not belong to it. The personal information included files relating to his personal life, but also files that had been shared with him on a confidential basis and were not the property of KXS.

[41] NXJ did provide undertakings and has offered that he will provide a statutory declaration.

[42] It is submitted that there is a very real risk of harm caused by a forensic examination, which will be caused to people who are not parties to this litigation, namely NXJ's partner and child who also use his computer and systems.

[43] In addition NXJ has access to personal information relating to the employees of his current employer who have a right to privacy of their information and for that information to be kept confidential.

Should a witness summons be issued?

[44] KXS has claimed that NXJ breached the confidentiality obligations he owed to it as a result of his copying a large number of files to a personal hard drive on his last day of employment. NXJ admits he did download the files but that he has subsequently deleted them.

[45] In considering whether or not a forensic examination is required for the Authority to determine the breach issue, I find the following persuasive:

- a. NXJ claims that the confidential information sent to him by HR professionals in other organisations was sent to him because of his personal connection and as such belongs to him.
 - i. I find that to the extent that any such information sent to NXJ at his KXS email address or otherwise provided to him whilst he was employed at KXS and downloaded and stored on KXS's computer system, it is not truly to be regarded as his personal information.

- ii. There is also the inference that as part of that information exchange, NXJ may have shared KXS's confidential information with other organisations, albeit on a confidential basis.
- b. The inconsistency of NXJ's evidence regarding which devices he transferred the KXS file information onto. I observe that an additional hard drive (in addition to the Microsoft Surface and personal computer) was mentioned by NXJ for the first time in the Investigation Meeting; and
- c. In response to KXS's request that NXJ agree to a forensic review process on 29 April 2022, NXJ destroyed the hard drive onto which he had downloaded the 640 files.
 - i. I understand that NXJ may have been concerned about the cost associated with that request, but he appeared to act precipitately by destroying the hard drive within the few days after receiving the email rather than waiting for a response to the email he sent to KXS on 6 May 2022.
 - ii. Although NXJ advised KXS in the email dated 6 May 2022 that he had permanently deleted all KXS files from the device, he did not inform it that he had destroyed the hard drive by means of a steel drill bit so it was no longer available for examination.

[46] I determine that it is appropriate a witness summons be issued requiring NXJ to attend a preliminary investigation meeting with his devices and platforms in order that these may be cloned.

Next Steps

[47] A case management call will take place with counsel to arrange a date for NXJ to attend the Authority offices with his devices and platforms for them to be cloned. The cloning will be undertaken by an independent forensic expert, identity to be agreed with counsel.

[48] The importance of ensuring NXJ's personal information is kept confidential is paramount throughout the process. To this end, the clones of NXJ's devices and platforms will sealed and kept securely until counsel have agreed with the Authority Member the search terms to be applied. This will either be at the Authority's premises, or with an independent solicitor.

[49] The cost of the forensic examination falls to KXS as the party applying for the summons.

Costs

[50] Costs are reserved pending the substantive outcome.

Eleanor Robinson
Member of the Employment Relations Authority